清华大学研究生公共课教材——数学系列

应用近世代数（第3版）学习指导和习题详解

胡冠章 编著

清华大学出版社

VISIT…

LANZAROTE Caliente.com

1560524

清华大学研究生公共课教材——数学系列

O153
O67

应用近世代数(第3版)学习指导和习题详解

胡冠章 编著

清华大学出版社
北京

内容简介

本书把《应用近世代数(第3版)》(胡冠章，王殿军. 清华大学出版社，2006，教育部优秀教材二等奖，普通高等教育"十一五"国家级规划教材)一书的习题全部做了详细解答，并收集了一些补充题. 每节开始有内容提要，便于学习. 每道题解答之前有分析，启发读者进行思考；每道题解完后有点评，指出该题的意义和是否还有其他解法等；使读者加深对近世代数内容的理解，掌握问题的分析方法和计算技巧，培养举一反三的能力. 本书可作为教学参考书，也适合自学之用. 适合数学和应用数学、计算机科学、信息科学、物理和化学等专业需要学习抽象代数知识的本科生、研究生和工程技术人员使用.

版权所有，侵权必究. 侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

应用近世代数(第3版)学习指导和习题详解/胡冠章编著. —北京：清华大学出版社，2012.10

(清华大学研究生公共课教材·数学系列)

ISBN 978-7-302-29573-0

Ⅰ. ①应… Ⅱ. ①胡… Ⅲ. ①抽象代数—研究生—教学参考资料 Ⅳ. ①O153

中国版本图书馆CIP数据核字(2012)第179293号

责任编辑：佟丽霞
封面设计：常雪影
责任校对：王淑云
责任印制：李红英

出版发行：清华大学出版社
　　网　址：http://www.tup.com.cn，http://www.wqbook.com
　　地　址：北京清华大学学研大厦A座　**邮　编**：100084
　　社 总 机：010-62770175　**邮　购**：010-62786544
　　投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
　　质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：三河市君旺印装厂
装 订 者：三河市新茂装订有限公司
经　销：全国新华书店
开　本：170mm×230mm　**印　张**：11.75　**字　数**：209千字
版　次：2012年10月第1版　**印　次**：2012年10月第1次印刷
印　数：1～4000
定　价：22.00元

产品编号：027288-01

前　　言

本书的目的不是简单地给出习题的解答，而是使读者加深对近世代数内容的理解，掌握问题的分析方法和计算技巧，培养举一反三的能力．因此采取了下面一些新的写法．

1．每节开始有内容提要，便于复习有关内容．这些内容提要并非简单重复书上的内容，而是经过简化、提炼与组织．对一些概念与定理用简洁的语言表达，便于记忆；或用式子表达，比较确切．例如，群的概念不再重复书上的详细表述，而是简化为：集合对运算满足封闭性、结合律、有单位元和逆元四个条件就构成群．另外，每节内容的顺序也有些改变以适合复习的特点．

2．每道题开始有分析，主要是指出该题的困难在哪里，可能用什么方法解决等．读者在解题之前先看一下分析，然后先自己去解．当解不下去时再去看解答部分，有思路了再自己做．做完后再详细对照一下解答，看每题后的点评．

3．每道题解完后有点评，指出该题的意义和是否还有其他解法等．有些题的点评还扩展了有关内容，例如，在第 4 章的 4.3-6 的点评中给出了一些有限域上的不可约与本原多项式的表，不仅可作为参考资料查阅，而且读者可自己进一步扩充知识点．

4．第 1～3 章是基本部分，都增加了一些补充题，作为综合练习和提高之用．

编者

2012 年 7 月

目　　录

第 1 章　引言和预备知识 …… 1
1.1　几类实际问题 …… 1
一、内容提要 …… 1
二、习题 1.1 详细解答 …… 1
1.2　集合与映射 …… 3
一、内容提要 …… 3
二、习题 1.2 详细解答 …… 3
1.3　二元关系 …… 8
一、内容提要 …… 8
二、习题 1.3 详细解答 …… 9
1.4　整数与同余方程 …… 12
一、内容提要 …… 12
二、习题 1.4 详细解答 …… 15
第 1 章补充题 …… 18

第 2 章　群论 …… 24
2.1　群的基本概念 …… 24
一、内容提要 …… 24
二、习题 2.1 详细解答 …… 26
2.2　子群 …… 31
一、内容提要 …… 31
二、习题 2.2 详细解答 …… 32
2.3　循环群和生成群，群的同构 …… 37
一、内容提要 …… 37
二、习题 2.3 详细解答 …… 38
2.4　变换群和置换群，Caylay 定理 …… 45
一、内容提要 …… 45
二、习题 2.4 详细解答 …… 47
2.5　子群的陪集和 Lagrange 定理 …… 52

一、内容提要 …… 52
二、习题 2.5 详细解答 …… 53
2.6 正规子群和商群 …… 57
一、内容提要 …… 57
二、习题 2.6 详细解答 …… 59
2.7 共轭元和共轭子群 …… 63
一、内容提要 …… 63
二、习题 2.7 详细解答 …… 66
2.8 群的同态 …… 74
一、内容提要 …… 74
二、习题 2.8 详细解答 …… 76
2.9 群对集合的作用,Burnside 引理 …… 81
一、内容提要 …… 81
二、习题 2.9 详细解答 …… 83
2.10 应用举例 …… 85
一、内容提要 …… 85
二、习题 2.10 详细解答 …… 86
2.11 群的直积与有限可换群 …… 90
一、内容提要 …… 90
二、习题 2.11 详细解答 …… 91
2.12 有限群的结构,Sylow 定理 …… 94
一、内容提要 …… 94
二、习题 2.12 详细解答 …… 95
第 2 章补充题 …… 97

第 3 章 环论 …… 105
3.1 环的基本概念 …… 105
一、内容提要 …… 105
二、习题 3.1 详细解答 …… 106
3.2 子环、理想和商环 …… 113
一、内容提要 …… 113
二、习题 3.2 详细解答 …… 115
3.3 环的同构与同态 …… 121
一、内容提要 …… 121

二、习题 3.3 详细解答 …… 122
3.4 整环中的因子分解 …… 130
一、内容提要 …… 130
二、习题 3.4 详细解答 …… 131
3.5 惟一分解整环 …… 133
一、内容提要 …… 133
二、习题 3.5 详细解答 …… 135
3.6 多项式分解问题 …… 139
一、内容提要 …… 139
二、习题 3.6 详细解答 …… 141
3.7 应用举例 …… 145
一、内容提要 …… 145
二、习题 3.7 详细解答 …… 145
第 3 章补充题 …… 146

第 4 章 域论 …… 149
4.1 域和域的扩张,几何作图问题 …… 149
一、内容提要 …… 149
二、习题 4.1 详细解答 …… 151
4.2 分裂域,代数基本定理 …… 156
一、内容提要 …… 156
二、习题 4.2 详细解答 …… 157
4.3 有限域,有限几何 …… 160
一、内容提要 …… 160
二、习题 4.3 详细解答 …… 162
4.4 单位根,分圆问题 …… 168
一、内容提要 …… 168
二、习题 4.4 详细解答 …… 170

第 5 章 方程根式可解问题简介 …… 172
5.1 多项式的伽罗瓦群 …… 172
一、内容提要 …… 172
二、习题 5.1 详细解答 …… 172

5.2 群的可解性和代数方程的根式求解问题 …………………… 176
一、内容提要 ………………………………………………………… 176
二、习题 5.2 详细解答 ……………………………………………… 177

参考文献 ……………………………………………………………………… 179

第 1 章　引言和预备知识

这一章的内容虽是准备部分，但非常重要，如果不熟悉，以后会处处受阻. 考虑到各人原有的基础不同，这一章的内容和习题适宜自学. 但不管是谁都应把内容和习题通读一遍，有重点地在某些内容上多加注意，例如关于整数的同余运算一定要熟悉起来.

1.1　几类实际问题

一、内容提要

本节的目的是提出一些可用近世代数解决的实际问题，以期引起读者的兴趣. 由于读者现在还未学习到有关内容，所以我们只能用初等的方法来做这些题，从中体会到问题的困难.

二、习题 1.1 详细解答

1.1-1　用两种颜色的珠子做成有 5 颗珠子的项链，问可做出多少种不同的项链？

分析　在学群论前我们没有一般的方法，只能用枚举法.

解　用笔在纸上画一下，用黑白两种珠子，分类进行计算：全白只 1 种，四白一黑 1 种，三白二黑 2 种，二白三黑 2 种，一白四黑 1 种，全黑只 1 种. 因此可得总共 8 种.

点评　读者不妨增加颜色数或珠子数再做做看，可以发现越来越难做，从而体会到必须寻找更高明的方法.

1.1-2　对正四面体的顶点用 2 种颜色着色，有多少种本质上不同的着色方法？

分析　我们可以用硬一点的纸做一个正四面体，也可在纸上画一个正四面体. 看看有多少种着色方法. 这里所说的本质上不同的着色方法，是指对两种着色不论怎样转动此正四面体它们都不能重合.

解　类似第 1 题，用枚举法可得 5 种.

点评　读者不妨增加颜色数再做做看，比项链问题更复杂，如没有更好的

方法是很难走远的.

1.1-3 有 4 个顶点的图共有多少个？其中互不同构的有多少个？

分析 复习一下图的概念，图一般指有标号的图，n 个点的图有 $2^{\binom{n}{2}}=2^{\frac{n(n-1)}{2}}$ 个. 但其中有很多是互相同构的，即不考虑点号，两个图可以重合就称为它们同构. 互不同构的图又叫无标号图. 求互不同构的图的个数是很难的问题，需要用群论方法.

解 由本节内容，有 4 个顶点的图共有 64 个图. 用分类计数的方法可得共有 11 个互不同构的图：无边的空图 1 个，一条边的图 1 个，有 2 条边的图有 2 个，有 3 条边的图有 3 个，有 4 条边的图有 2 个，有 5 条边的图有 1 个，有 6 条边的图有 1 个.

点评 读者不妨算一下有 5 个顶点的图共有多少个有标号图，有多少个互不同构的图. 虽只增加一个点，但难度有很大的提高.

1.1-4 如何用圆规 5 等分一个圆周？

分析 可先作一个单位圆，设其半径长度为 1，问题变成如何求出五边形的边长.

解 用初等数学的方法求五边形的边长：作一个顶角为 36°、腰长为 1 的等腰三角形，设底边长为 a，则 a 就是十边形的边长，以 a 为半径以单位圆周上任意一点为圆心在圆周上交出两点，则这两点之间的距离就是五边形的边长. 那么 a 怎么求呢？只要在那个等腰三角形上作一条辅助线：底角的角平分线，再利用相似三角形边长成比例的关系，可得 $a=\frac{\sqrt{5}-1}{2}$，分别以 1 和 2 作直角边，斜边就是$\sqrt{5}$，所以 a 就可作出了.

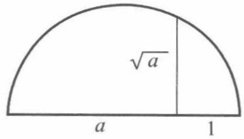


图 1.1

点评 由于一个数的开平方可以在圆上作出(见图 1.1，即主教材图 4.2)，所以，如果正 n 边形的边长，可由某个有理数经过有限次开平方与四则运算求得，则就可 n 等分一个圆. 但这是否是可 n 等分一个圆周的必要条件呢？我们将在第 4 章中详细讨论此问题.

1.1-5 如何用根式表示 3 次和 4 次代数方程的根？

查看数学手册. 因公式较复杂，不在这里列出了.

点评 从手册可见，对 3 次和 4 次代数方程可通过几步表示它的根，每一步都是根式表示式. 而对于 5 次以上的某些代数方程，伽罗瓦证明了对某些 5 次方程不能用根式表示它的根. 我们将在第 5 章中讨论此问题.

1.2 集合与映射

一、内容提要

由于集合的概念太基本了，没有必要从头复习，我们只是强调和补充一些东西.

1. 集合

- **集合的记号**：本书用大写字母表示集合. $|A|$表示集合 A 的元素的个数，称为基数. 用$|A|<\infty$表示有限集.

整数集合记作：$\mathbb{Z}$. 正整数(即自然数)集合记作：$\mathbb{Z}^+$(自然数是否包含 0，有不同的说法，高等教育出版社出版的《数学手册》把自然数定义为正整数). 非负整数的集合无专门的记号. 非零整数的集合记作：$\mathbb{Z}^*$. 类似的，对有理数有记号：$\mathbb{Q}$，$\mathbb{Q}^+$，$\mathbb{Q}^*$；对实数有记号：$\mathbb{R}$，$\mathbb{R}^+$，$\mathbb{R}^*$；对复数有记号：$\mathbb{C}$，$\mathbb{C}^*$.

- **集合 A 的幂集**记作：$\mathscr{P}(A)=2^A=\{A$ 的所有子集的集合$\}$. 当$|A|<\infty$时有$|2^A|=2^{|A|}$.
- **包含与排斥原理**：设 $A_1,A_2,\cdots,A_n$ 是集合 S 的有限子集，则

$$\left|\bigcap_{i=1}^n A_i\right|=\sum_{i=1}^n|A_i|-\sum_{1\leqslant i<j\leqslant n}|A_i\cup A_j|+\cdots+(-1)^{n-1}\left|\bigcup_{i=1}^n A_i\right|,$$

$$\left|\bigcup_{i=1}^n A_i\right|=\sum_{i=1}^n|A_i|-\sum_{1\leqslant i<j\leqslant n}|A_i\cap A_j|+\cdots+(-1)^{n-1}\left|\bigcap_{i=1}^n A_i\right|.$$

当并集的基数比交集的基数容易求时，用第一个公式. 反之，用第二个公式.

2. 映射

集合 A 到集合 B 的映射记作：$f:x\mapsto f(x)(A\to B)$.

- f 是单射$\Leftrightarrow f(x_1)=f(x_2)\Rightarrow x_1=x_2$.
- f 是满射$\Leftrightarrow f(A)=B$.
- f 是双射$\Leftrightarrow f$ 既是单射又是满射.
- f 可逆$\Leftrightarrow f$ 是双射.

二、习题 1.2 详细解答

1.2-1 设$|A|<\infty$，用二项式定理证明：$|2^A|=2^{|A|}$.

分析 二项式定理为：$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b^2+\cdots+b^n$. 求

幂集的元素个数如何与二项式定理联系起来呢？我们从二项式系数$\binom{n}{k}$入手，它是从 n 个元素中取 k 个元素的取法，正好是 k 元子集的个数，而全部子集的个数正好就是这些二项式系数之和.

证　设 $A=\{a_1,a_2,\cdots,a_n\}$，由于 A 中 k 元子集的个数等于二项式系数$\binom{n}{k}$，于是把它们从 $k=1$ 到 $k=n$ 加起来，再加一个空集，所以

$$|2^A|=1+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}=(1+1)^n=2^n=2^{|A|}.$$

点评　证明该公式方法至少有以下几种：

证法1　如主教材1.2.2(指主教材的节号，下同.例子号，定理号等均指主教材中的.)中所说：每一个元素有在子集中与不在子集中2种可能，因而共有 2^n 种可能，每一种可能对应一个子集，所以共有 2^n 个子集.

证法2　用二项式定理.

证法3　利用主教材1.2.6节中公式：$|B^A|=|B|^{|A|}$. 令 $A=\{a_1,a_2,\cdots,a_n\}$，$B=\{0,1\}$，则每一个 A 到 B 的映射对应一个子集，所以全部子集的个数为 $|B^A|=|B|^{|A|}=2^n$.

1.2-2　一个班有93%的人是团员，80%的人担任过社会工作，70%的人受过奖励，问：

(1) 受过奖励的团员至少占百分之几？

(2) 三者兼而有之的人至少占百分之几？

分析　该题是求几个集合的交集的基数，可用包含与排斥原理得到比较精确的结果.

解　设 A 为团员的集合，B 为担任过社会工作的人的集合，C 为受过奖励的人的集合，则由包含与排斥原理，可得

(1) $|A\cap C|=|A|+|C|-|A\cup C|\geqslant 93+70-100=63$，
所以受过奖励的团员至少占63%.

(2) $|A\cap B\cap C|=|A|+|B|+|C|-|A\cup B|-|B\cup C|-|A\cup C|+|A\cup B\cup C|$，由于 $|A\cup B\cup C|-|A\cup B|\geqslant 0$，所以

$$\begin{aligned}|A\cap B\cap C|&\geqslant|A|+|B|+|C|-|B\cup C|-|A\cup C|\\&\geqslant 93+80+70-100-100=43.\end{aligned}$$

故三者兼而有之的人至少占43%.

点评　该题主要是复习集合运算的包含与排斥原理. 对于集合个数较少时，可用画图的方法来确定.

1.2-3 在不大于1000的正整数中，求：

(1) 不能被5,6,8中任何一个整数整除的个数.

(2) 既非平方数也非立方数的个数.

分析 利用包含与排斥原理，参考主教材例1.2.1.

解 (1) 设 $X=[1,1000]$ 表示1到1000的所有整数，$A=\{x\mid x\in X\&5\mid x\}$，即为 X 中能被5整除的所有整数的集合，$B=\{x\mid x\in X\&6\mid x\}$，$C=\{x\mid x\in X\&8\mid x\}$. 则

$$|A|=\frac{1000}{5},\quad |B|=\left\lfloor\frac{1000}{6}\right\rfloor,\quad |C|=\left\lfloor\frac{1000}{8}\right\rfloor,$$

并可求出

$$|A\cap B|=\left\lfloor\frac{1000}{5\times 6}\right\rfloor=33,\quad |B\cap C|=\left\lfloor\frac{1000}{[6,8]}\right\rfloor=41,$$

$$|A\cap C|=\left\lfloor\frac{1000}{5\times 8}\right\rfloor=25,\quad |A\cap B\cap C|=\left\lfloor\frac{1000}{[5,6,8]}\right\rfloor=8,$$

其中[6,8]和[5,6,8]是最小公倍数的记号. 记号 $\lfloor x\rfloor$ 表示 x 的下整数，$\lceil x\rceil$ 表示 x 的上整数. 所以所求的个数为

$$\begin{aligned}|X|-|A\cup B\cup C|&=1000-|A|-|B|-|C|+|A\cap B|\\&\quad+|B\cap C|+|A\cap C|-|A\cap B\cap C|\\&=1000-200-166-125+33+41+25-8\\&=600.\end{aligned}$$

(2) 设 A 为 X 中平方数的个数，B 为 X 中立方数的个数，则

$$|A|=\lfloor\sqrt{1000}\rfloor=31,\quad |B|=\lfloor\sqrt[3]{1000}\rfloor=10,$$

$$|A\cap B|=\lfloor\sqrt[6]{1000}\rfloor=3.$$

所以所求的个数为

$$\begin{aligned}|X|-|A\cup B|&=1000-|A|-|B|+|A\cap B|\\&=1000-31-10+3\\&=962.\end{aligned}$$

点评 根据题意，首先确定是求集合的交还是并，然后利用包含与排斥原理.

1.2-4 设 $|A|=m$，$|B|=n$，求：

(1) A 到 B 的单射有多少个？

(2) 当 $m=3$，$n=2$ 时，求 A 到 B 的满射有多少个？

分析 $f: A\to B$ 是单射 $\Leftrightarrow |f(A)|=|A|$，因而 $|A|\leqslant|B|$.

$f: A\to B$ 是满射 $\Leftrightarrow |f(A)|=|B|$，因而 $|A|\geqslant|B|$.

解 (1) 当 $m>n$ 时，显然不存在 A 到 B 的单射.

当 $m\leqslant n$ 时，由于单射的像必是 B 中的某个 m-子集，且和子集元素的次序有关，由此可得 A 到 B 的单射个数为以下从 m 个元素中选取 n 个元素的选排列数：

$$P(m,n)=m(m-1)\cdots(m-n+1).$$

(2) 当 $m<n$ 时，显然不存在 A 到 B 满射.

当 $m\geqslant n$ 时，存在 A 到 B 满射. 对于 $m=3,n=2$，设 $A=\{a_1,a_2,a_3\}$，$B=\{0,1\}$，我们知道 A 到 B 全部映射数为8，非满射只有2个，所以 A 到 B 的满射有6个.

点评 对一般情形，求满射数的问题可参看[4]p. 52-53.（参考文献的页码是本书后所附的参考文献，下同.）

1.2-5 证明实数区间 $(0,1)$ 与 $(-\infty,+\infty)$ 等势.

分析 关键是在这两个集合之间找一个双射.

证 作映射 $f:x\mapsto \ln\dfrac{x}{1-x}$. 可证 f 是单射：任取 $x_1,x_2\in(0,1)$，有

$$\ln\frac{x_1}{1-x_1}=\ln\frac{x_2}{1-x_2}\Rightarrow\frac{x_1}{1-x_1}=\frac{x_2}{1-x_2}\Rightarrow x_1-x_1x_2$$
$$=x_2-x_1x_2\Rightarrow x_1=x_2.$$

所以 f 是单射.

再证 f 是满射：任取 $y\in(-\infty,+\infty)$，令 $y=\ln\dfrac{x}{1-x}$，可解出 $x=\dfrac{e^y}{1+e^y}\in(0,1)$ 使 $f(x)=y$，所以 f 是满射.

综上，f 是双射，因此 $(0,1)$ 与 $(-\infty,+\infty)$ 等势.

点评 可以找到很多满足要求的映射，读者试另找一个双射.

1.2-6 设 f 是 A 到 B 的一个映射，$S\subseteq A$，举例说明 $f^{-1}[f(S)]=S$ 是否成立?

注意 这里的记号 f^{-1} 并非指 f 的逆，f 不一定可逆. $f^{-1}[T]$ 表示 T 的全原像.

解 不一定成立.

成立的情况：显然当 f 可逆时，$f^{-1}[f(S)]=S$ 成立. 实际上，只要 f 是单射，式子就成立：$\forall x\in S$，设 $f(x)=y$，由于 f 是单射，y 的原像只有 x，即 $f^{-1}[f(x)]=x$，所以 $f^{-1}[f(S)]=S$.

不成立的情况：只要举一个 f 不是单射的例子. 例如：$f:x\mapsto x^2,\mathbb{R}\to\mathbb{R}$. 取 $S=\{1\}$，则 $f(S)=\{1\}$，但 $f^{-1}[f(S)]=f^{-1}(1)=\{-1,1\}\neq S$.

点评 可以一般的证明：$f^{-1}[f(S)]=S$ 成立的充分必要条件是 f 是单射.

1.2-7 设 $|A|<\infty$，$f:A\to A$，证明以下三个命题等价：

(1) f 是单射； (2) f 是满射； (3) f 可逆.

分析 这个题的结论很重要，即有限集上的单射、满射与双射都是互为充要条件. 证明方法并不复杂.

证 用循环证法：

(1)⇒(2)：因为 f 是单射，且 A 是有限集，故有 $|f(A)|=|A|$. 所以 f 是满射.

(2)⇒(3)：因为 f 是满射，故有 $f(A)=A$. 下面用反证法证明 f 是单射：假设 f 不是单射，由于 A 是有限集，必故有 $|f(A)|<|A|$. 与 f 是满射矛盾，所以 f 是单射. 因而 f 是双射，即可逆.

(3)⇒(1)：显然.

点评 我们再强调一下，对有限集这个结论很重要！即有限集上的单变换必是满变换，也必是双变换和可逆变换. 通常遇到有限集的问题我们要充分利用有限性使问题简化，甚至可列出所有的元素来进行分析.

1.2-8 设 $A\neq\varnothing$，证明不存在 A 到它的幂集 $\mathscr{P}(A)$ 的双射.

分析 如果 A 是有限集，这个结论是显然的. 因为 $\mathscr{P}(A)$ 的元素个数多于 A 的元素个数，因此不存在 A 到 $\mathscr{P}(A)$ 的双射. 但对于无限集，就不能用用这种方法证明了. 下面的证法有特殊的技巧.

证 用反证法.

假设存在 A 到 $\mathscr{P}(A)$ 的双射 $f:x\mapsto f(x)=S_x\in\mathscr{P}(A)$. 在 A 中取一个满足以下条件的子集：

$$T=\{x\mid x\in A\,\&\,x\notin S_x\}.$$

$T\in\mathscr{P}(A)$，由于 f 是满射，存在 $a\in A$ 使 $f(a)=S_a=T$，现我们分析 a 是否在 T 中？

若 $a\in T$，根据 T 的定义有 $a\notin S_a$，即 $a\notin T$，矛盾.

若 $a\notin T$，即 $a\notin S_a$，根据 T 的定义有 $a\in T$，也矛盾.

所以不可能有这样的双射存在.

点评 是否有其他的证明方法呢？如有更简单的证明方法请发 Email 至 hugz@tsinghua.edu.cn.

1.3　二元关系

一、内容提要

1. 二元运算和代数系

我们从小学开始所做的运算大多是两个数的运算，但不太关心数的范围的变化. 例如，两个正整数相减，其结果可能跑出正整数的范围；一个整数开平方，其结果不仅可能跑出整数的范围，而且可能跑出有理数的范围. 在近世代数中，不管做什么样的运算，我们始终念念不忘是在什么集合里进行，其结果是否还在这个集合里？而且只有其结果仍在原集合的运算称为二元运算，具体定义如下：

- **二元运算**：设 S 为非空集合，则映射 $f:S\times S\rightarrow S$ 就称为 S 中的一个二元运算. 其最主要之点是满足封闭性和惟一性.
- **代数系**：定义了一个或几个二元运算的集合就称为一个代数系. 对不同的集合定义不同的运算就得到不同的代数系，例如群，环，域等. 代数系是近世代数的基本舞台.

2. 二元关系和等价关系

我们从小学开始就知道相等、大于和小于等关系，后来学几何又知道三角形的全等、相似等关系，在线性代数里又有矩阵的相似、相合等关系. 这些都是二元关系. 其中最重要的是等价关系.

- **二元关系**：在两个集合 A 和 B 的元素之间如果有一个规则 R，$\forall a\in A$，$\forall b\in B$ 可判断 aRb(a 与 b 符合规则 R)，或 $aR'b$(a 与 b 不符合规则 R). 则规则 R 就称为集合 A 和 B 的元素之间的一个二元关系.
- **等价关系**：在同一个集合里，一个二元关系如果满足3个条件：反身性，对称性和传递性. 则此二元关系称为此集合中的一个等价关系，等价关系记作 $\sim$、$=$ 、$\equiv$ 等.
- **等价类及其代表元**：设集合 A 中的一个等价关系为 $\sim$，则子集 $\bar{a}=\{x\mid x\sim a\}$ 称为以 a 为代表的等价类，它的记号有：$\tilde{a}$，$[a]$ 等，以 $\bar{a}$ 最简单，本书主要采用此记号.
- **商集**：A 中等价类的集合，记作 $A/\sim=\{\bar{a}\mid a\in A\}$，称为 A 模 $\sim$ 的商集. 它是 A 的幂集的一个子集.
- **一个重要的等价关系——同余关系**(非常重要!)：先在整数集合 $\mathbb{Z}$ 中

定义一个二元关系称为整除关系：$a|b \Leftrightarrow \exists c \in \mathbb{Z}$ 使 $b=ac$. 然后可定义两整数的同余关系.

整数集合$\mathbb{Z}$中模 n 的同余关系记作：$\equiv(\text{mod } n)$，定义为

$$a \equiv b(\text{mod } n) \Leftrightarrow n \mid (a-b).$$

这个等价关系的记号有点复杂和特殊，"a 与 b 模 n 同余"习惯记作 $a \equiv b(\text{mod } n)$. 整数模 n 的同余类：$\bar{a}=\{a+qn|q\in\mathbb{Z}\}$. a 是 $\bar{a}$ 的代表元，代表元不是惟一的. 若取代表元满足：$0\leqslant a<n$，则称它是**正则代表元**，是惟一确定的.

有的书把同余类记作：$[a]=\{a+qn|q\in\mathbb{Z}\}$.

整数模 n 的商集：$\mathbb{Z}_n=\mathbb{Z}/\equiv(\text{mod } n)=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$. 称为整数模 n 的同(剩)余类集合.

二、习题 1.3 详细解答

1.3-1 $A=\{1,2,3,4,5\}$，在 2^A 中定义二元关系$\sim$：$S\sim T \Leftrightarrow |S|=|T|$. 证明$\sim$是等价关系，并写出等价类和商集 $2^A/\sim$.

分析 此题虽然简单，但对还不太熟悉等价类和商集的读者来说，还是应认真做一下.

证 易证$\sim$满足等价关系的三个条件，反身性，$|S|=|S|\Rightarrow S\sim S$；对称性：$S\sim T\Rightarrow |S|=|T|\Rightarrow T\sim S$；传递性：$S\sim T, T\sim U\Rightarrow |S|=|T|=|U|\Rightarrow S\sim U$.

等价类为：$\overline{\varnothing}=\{\varnothing\}$，$\overline{\{1\}}=\{\{1\},\{2\},\{3\},\{4\},\{5\}\}$，

$$\overline{\{1,2\}}=\{\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\{3,5\},\{4,5\}\},$$

$$\overline{\{1,2,3\}}=\{\{1,2,3\},\{1,2,4\},\{1,2,5\},\cdots,\{3,4,5\}\},$$

$$\overline{\{1,2,3,4\}}=\{\{1,2,3,4\},\cdots,\{2,3,4,5\}\},$$

$$\bar{A}=\{A\}.$$

商集为 $2^A/\sim=\{\overline{\varnothing},\overline{\{1\}},\overline{\{1,2\}},\overline{\{1,2,3\}},\overline{\{1,2,3,4\}},\bar{A}\}$.

点评 这是概念题，虽然简单，但必须仔细写一写，以加深印象，并熟悉表示方法.

1.3-2 $S=\{0,1,\cdots,n\}$，$f:A\mapsto \text{r}(A)(M_n(\mathbb{R})\to S)$. 求由 f 所决定的等价关系，并决定等价类和商集.

分析 本题是把所有实 n 阶矩阵按秩分类，注意把等价类的代表元写得简单一些.

解　f 所决定的等价关系～为：$A\sim B\Leftrightarrow \mathrm{r}(A)=\mathrm{r}(B)$. 易证～满足等价关系的三个条件(略). 在秩为 k 的等价类中最简单的矩阵为 $\begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}$，所以得到

等价类：$\overline{\begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}} = \{A \mid A \in M_n(\mathbb{R}), \mathrm{r}(A) = k\}, k = 0,1,\cdots,n.$

商　集：$M_n(\mathbb{R})/\sim = \left\{ \overline{\begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}} \middle| k = 0,1,\cdots,n \right\}.$

点评　矩阵集合是近世代数的重要研究对象，我们必须对它很熟悉.

1.3-3　在 $M_n(\mathbb{C})$ 中定义二元关系～：$A\sim B\Leftrightarrow$ 存在可逆阵 P 使 $PAP^{-1}=B$. 证明～是等价关系，并决定等价类和商集.

证　由于所定义的二元关系～是矩阵的相似关系，在线性代数中已经证明过它是等价关系. 等价类中最简单的代表元是约当标准形，但是由于约当标准形很难全部表达出来，所以无法再继续下去.

点评　有些问题中等价类的代表元很难表达，因而商集也写不出来，我们只要从概念上理解清楚就行了.

1.3-4　设 S 为 n 阶实对称矩阵的集合，定义二元关系～：$A\sim B\Leftrightarrow$ 存在可逆阵 C 使 $C^{\mathrm{T}}AC=B$，证明～是等价关系，并求 $|S/\sim|$.

分析　这是线性代数中的矩阵相合关系，已证明过是等价关系，这里不妨再证一下. 由于实对称矩阵可通过相合变换化为对角元素为 1，或 -1，或 0 的规范形，所以等价类的最简单的代表元就是规范形.

证与解　反身性：$I^{\mathrm{T}}AI=A\Rightarrow A\sim A$. 对称性：$A\sim B\Rightarrow C^{\mathrm{T}}AC=B\Rightarrow (C^{-1})^{\mathrm{T}}BC^{-1}=A\Rightarrow B\sim A$. 传递性：$A\sim B, B\sim C\Rightarrow \exists P,Q$: $P^{\mathrm{T}}AP=B$, $Q^{\mathrm{T}}BQ=C\Rightarrow (PQ)^{\mathrm{T}}A(PQ)=C\Rightarrow A\sim C$.

在线性代数中我们知道实对称矩阵可用可逆矩阵化为规范形，所以得商集为

$$S/\sim = \left\{ \overline{\begin{bmatrix} -I_k & 0 & 0 \\ 0 & I_l & 0 \\ 0 & 0 & 0 \end{bmatrix}} \middle| 0 \leqslant k+l \leqslant n \right\}.$$

其元素个数可以这样来计算：先看规范形中 -1 的个数，如有 k 个 -1，则对应 $n-k+1$ 个不同的矩阵，因而总数为

$$\sum_{k=0}^{n}(n-k+1),$$

再变换一下和式中的变量，得

$$|S/\sim| = \sum_{m=0}^{n}(m+1) = \frac{(n+1)(n+2)}{2}.$$

点评 因为实对称矩阵的相合标准形可取对角元素为-1,1或0的规范形,因此商集元素的个数就是不同规范形的个数.

1.3-5 举一个偏序集但不是全序集的例子,并画出它的Hasse图.

解 考虑到画图的方便,可举有限集的例子,例如:有限集的幂集对包含关系所构成的偏序集,有限整数集对整除关系所构成的偏序集.

详解略.

点评 此题虽简单,但对初学者还是要认真写一写.

1.3-6 已知两个偏序集的Hasse图形如下,分别写出它们的偏序集及偏序关系.

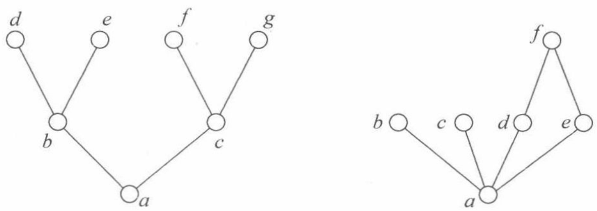
解 按偏序的定义,可直接列出所有有序的关系的元素对就可以了.

(a) 的偏序集可表为:$(S,\leqslant)$,其中

$$S=\{a,b,c,d,e,f,g\},\quad \leqslant=\{a<b,a<c,b<d,b<e,c<f,c<g\}.$$

(b) 的偏序集可表为:$(T,\leqslant)$,其中

$$T=\{a,b,c,d,e,f\},\quad \leqslant=\{a<b,a<c,a<d,a<e,d<f,e<f\}.$$



(a) (b)

图 1.2

1.3-7 用两种方法定义$\mathbb{Z}$的序,使它成为一个良序集.

分析 良序集要求任何两个元素都有序,且任何子集都有最小元.首先要使整个集合有最小元,我们可以把整数轴选择不同的点把左边折过来到右边,从而得到不同的良序集.

解 (1) 取0作为最小元,在$\mathbb{Z}$中定义偏序关系$\leqslant$为

$$a<b \Leftrightarrow |a|<|b| \quad 或 \quad |a|=|b| \quad 且 \quad a<b,$$
$$a=b \Leftrightarrow a=b.$$

其中右边的$<$和$=$为普通的小于和等于.按此序排列的整数集合为

$$0,-1,1,-2,2,-3,3,\cdots.$$

下面证明$(\mathbb{Z},\leqslant)$是良序集:设S是$(\mathbb{Z},\leqslant)$的任一非空子集,令

$$A=\{|x| \mid x\in S\},$$

则 A 是非负整数集的子集，由非负整数集的良序性，A 有最小元 a，显然，a(或 $-a$)也是 S 的最小元，所以($\mathbb{Z}$，$\leqslant$)是良序集.

(2) 取1作为最小元，在 $\mathbb{Z}$ 中定义偏序关系 $\leqslant$ 为

$$a < b \Leftrightarrow |a-1| < |b-1| \text{ 或 } |a-1| = |b-1| \text{ 且 } a < b,$$
$$a = b \Leftrightarrow a = b.$$

其中右边的 $<$ 和 $=$ 为普通的小于和等于. 按此序排列的整数集合为

$$1,0,2,-1,3,-2,4,-3,5,\cdots.$$

良序性证明类似(1).

点评　以上两种方法比较类似，是否有其他的差别较大的方法?

1.4　整数与同余方程

一、内容提要

虽然我们对整数已经很熟悉了，但这一节内容的重要性无论怎样强调都不过分. 可以说，全书的内容都以本节内容为基础，是它的推广与发展.

1. 整数运算的几个重要公式(非常重要!)

- **带余除法定理**：$a,b\in\mathbb{Z}$，$b\neq 0$，则存在惟一的 $q,r\in\mathbb{Z}$ 满足

$$a = qb + r \quad \text{且} \quad 0 \leqslant r < |b|.$$

并记作

$$a \bmod b = r, \quad \text{或} \quad a(\bmod b) = r,$$

称 ***a* 模 *b* 的余为 *r***. 用前面给出的同余的概念有 $a\equiv r(\bmod b)$. 这里用了两个略有不同的记号，它们的区别是：$a\bmod b$ 是一种运算，给出惟一的结果，用等号表示. 而 $\equiv(\bmod b)$ 给出的是两个整数之间的关系，用恒等号表示. 例如，

$$7\bmod 5 = 2, \qquad \text{或 } 7(\bmod 5) = 2.$$
$$7 \equiv 2 \equiv -3 \equiv \cdots(\bmod 5).$$

显然有

$$a_1 \equiv a_2(\bmod b) \Leftrightarrow a_1 \bmod b = a_2 \bmod b,$$

所以两个整数模 b 同余就是它们模 b 的余相同，这就是同余这个名词的意义.

注　记号 $a\bmod b$ 是本书根据近代文献引入的一个新的记号，在实际应用中很有用. 在本书中，当强调求余数时用等号"="，当强调表示两个数的同余关系时用恒等号"≡".

- **算术基本定理**：每一个大于1的正整数 n 可分解为素数的幂之积：

$$n = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_s^{\varepsilon_s},$$

其中 $p_1,p_2,\cdots,p_s$ 是不同的素数，此式称为**整数的标准分解式**.

利用算术基本定理可计算出正整数 n 的因子数为 $(\varepsilon_1+1)(\varepsilon_2+1)\cdots(\varepsilon_s+1)$.

2. 最大公因子

- **最大公因子定义**：设 $a,b\in\mathbb{Z}$，不全为 0，若有 $d\in\mathbb{Z}^*$ 满足：(1) $d|a$ 且 $d|b$；(2) 如果有 d' 满足 $d'|a$ 且 $d'|b$，则 $d'|d$. 则称 d 是 a 与 b 的最大公因子. 当 d 是 a 与 b 的最大公因子时，$-d$ 也是 a 与 b 的最大公因子，我们把正的最大公因子记作 (a,b).

类似可定义最小公倍数，a 与 b 的正的最小公倍数记作 $[a,b]$.

- **最大公因子定理**(或 Bezout 公式)：设 $a,b\in\mathbb{Z}$，不全为 0，a 与 b 的最大公因子为 $d=(a,b)$，则存在 $p,q\in\mathbb{Z}$ 使

$$pa+qb=d.$$

- **有关最大公因子的计算方法**：

(1) **利用算术基本定理法**：取 a 与 b 的标准分解式中相同的素数的最低次幂作出的乘积就是 $d=(a,b)$.

(2) **辗转相除法**：先用辗转相除法求出 $d=(a,b)$，再用回代法得到 p,q；或可用大衍求一术公式编程等.

- **最大公因子与最小公倍数的关系**：$(a,b)[a,b]=ab$.
- **素数与互素的性质**：

(1) $(a,b)=1\Leftrightarrow\exists\, p,q\in\mathbb{Z}:pa+qb=1$.

(2) $a|bc$ 且 $(a,b)=1\Rightarrow a|c$.

(3) 设 p 为素数，则有 $p|ab\Rightarrow p|a$ 或 $p|b$.

(4) $(a,b)=1$ 且 $(a,c)=1\Rightarrow(a,bc)=1$.

(5) $a|c,b|c$ 且 $(a,b)=1\Rightarrow ab|c$.

- **欧拉 φ-函数**：设大于 1 的正整数 $n=p_1^{\varepsilon_1}p_2^{\varepsilon_2}\cdots p_s^{\varepsilon_s}$，则小于 n 并与 n 互素的正整数的个数为：

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right).$$

并有性质：当 $(m,n)=1$ 时有 $\varphi(mn)=\varphi(m)\varphi(n)$.

3. 同余方程

- **一次同余方程**：$ax\equiv b\pmod m$ ($a\not\equiv 0\pmod m$) 有解的充分必要条件是 $(a,m)|b$. 且有解时通解为

$$x \equiv pb_1 \pmod{m_1} \quad 或 \quad x = pb_1 + km_1, \quad k \in \mathbb{Z},$$

其中 b_1, m_1 的意义如下：

$$a = a_1(a,m), \quad b = b_1(a,m), \quad m = m_1(a,m),$$

p 满足：$pa_1 + qm_1 = 1$.

因此一次同余方程 $ax \equiv b \pmod{m}$ ($a \not\equiv 0 \pmod{m}$) 的**求解步骤**为

(1) 求 $d = (a,m)$，若 $d \mid b$，则方程有解.

(2) 求 a_1, b_1, m_1：$a_1 = a/d$，$b_1 = b/d$，$m_1 = m/d$.

(3) 求 p：$pa_1 + qm_1 = 1$.

(4) 得通解为 $x \equiv pb_1 \pmod{m_1}$ 或 $x = pb_1 + lm_1$，$l \in \mathbb{Z}$.

- **一次同余方程组的求解方法——孙子定理.**

由于一次同余方程组中每个同余方程必须有解，故每个同余方程可表示为解出形式，所以一次同余方程组可表示为以下形式：

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \quad \vdots \\ x \equiv b_k \pmod{m_k}. \end{cases} \tag{1.1}$$

定理(孙子定理)　设 $m_1, m_2, \cdots, m_k$ 为 k 个两两互素的正整数，令

$$M = m_1 m_2 \cdots m_k = m_1 M_1 = m_2 M_2 = \cdots = m_k M_k,$$

则同余方程组的一般解为

$$x \equiv b_1 c_1 M_1 + b_2 c_2 M_2 + \cdots + b_k c_k M_k \pmod{M}, \tag{1.2}$$

其中 c_i 是满足同余方程 $M_i x \equiv 1 \pmod{m_i}$ 的一个特解，$i = 1, 2, \cdots, k$.

由此得**求同余方程组的一般解的步骤**为

(1) 求 $M = m_1 m_2 \cdots m_k$，$M_i = M/m_i$，$i = 1, 2, \cdots, k$.

(2) 求同余方程 $M_i x \equiv 1 \pmod{m_i}$ 的一个特解 c_i，$i = 1, 2, \cdots, k$.

(3) 得同余方程组(1.1)的一般解为

$$x \equiv b_1 c_1 M_1 + b_2 c_2 M_2 + \cdots + b_k c_k M_k \pmod{M}.$$

- 当 $k = 2$ 时，同余方程组为

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \end{cases} \tag{1.3}$$

$(m_1, m_2) = 1$. 若 $pm_1 + qm_2 = 1$，则方程组(1.3)的解为

$$x \equiv b_1 q m_2 + b_2 p m_1 \pmod{m_1 m_2}. \tag{1.4}$$

注意脚标对应关系的特点. 公式(1.4)是公式(1.2)的特殊情况.

类似可研究二次同余方程 $x^2 \equiv a \pmod{n}$ 的解的问题(以后将会学到).

二、习题 1.4 详细解答

1.4-1　$a=493, b=391$，求(a,b)，$[a,b]$和 p,q 使 $pa+qb=(a,b)$.

分析　可用两种方法来求最大公因子：辗转相除法和大衍求一术. 然后用公式$(a,b)\cdot[a,b]=ab$ 求出$[a,b]$.

解　**方法 1**　辗转相除法. 列以下算式：

$$a = 1\times b+102,$$
$$b = 3\times 102+85,$$
$$102 = 1\times 85+17,$$
$$85 = 5\times 17.$$

由此得到

$$(a,b) = 17,\quad [a,b] = \frac{ab}{17} = 11339.$$

然后回代：$17=102-85=102-(b-3\times 102)=-b+4\times 102=-b+4(a-b)=4a-5b$. 所以得

$$p = 4,\quad q =-5.$$

方法 2　大衍求一术.

公式与计算表格如下：

$$r_{k-2} = q_k r_{k-1}+r_k,\quad (\text{带余除法})r_{-1} = a, r_0 = b \text{ 且 } a > b;$$
$$c_k = q_k c_{k-1}+c_{k-2},\quad c_{-1} = 1, c_0 = 0;$$
$$d_k = q_k d_{k-1}+d_{k-2},\quad d_{-1} = 0, d_0 = 1.$$

一直计算到 $r_n\neq 0, r_{n+1}=0$，则

$$d = (a,b) = r_n,$$
$$p = (-1)^{n-1}c_n,\quad q = (-1)^n d_n.$$

k	q_k $r_{k-2}=q_k r_{k-1}+r_k$	r_k	c_k $c_k=q_k c_{k-1}+c_{k-2}$	d_k $d_k=q_k d_{k-1}+d_{k-2}$
-1		$a=493$	1	0
0		$b=391$	0	1
1	1	102	1	1
2	3	85	3	4
$3(n)$	1	17	4	5
$4(n+1)$	5	0		

由此求得 $n=3$，

$$d = (a,b) = 17,$$

$$p=(-1)^{n-1}c_n=c_3=4,\quad q=(-1)^n d_n=-d_3=-5.$$

点评 两个方法比较：辗转相除法比较直观，容易记忆，适合手算；大衍求一术公式比较复杂，不易记忆，但适合计算机编程.

1.4-2 求 $n=504$ 的标准分解式和 $\varphi(n)$.

分析 求标准分解式的方法可用素数来除，由小到大进行：2,3,5,⋯.

解 作以下计算：

$$\begin{array}{r|l} 2 & 504 \\ \hline 2 & 252 \\ \hline 2 & 126 \\ \hline 3 & 63 \\ \hline 3 & 21 \\ \hline & 7 \end{array}$$

所以 $504=2^3\times3^2\times7$.

$$\varphi(504)=504\times\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)=144.$$

点评 只是简单地套公式，读者可以自己再举些例子算一算.

1.4-3 团体操表演过程中要求队伍变换成10行、15行、18行、24行时，均成长方形，问需要多少人？

分析 这是一个求最小公倍数的问题.

解 求最小公倍数：作以下算式

$$\begin{array}{r|rrrr} 5 & 10, & 15, & 18, & 24 \\ \hline 2 & 2 & 3 & 18 & 24 \\ \hline 3 & 1 & 3 & 9 & 12 \\ \hline & 1 & 1 & 3 & 4 \end{array}$$

得

$$[10,15,18,24]=5\times2\times3\times3\times4=360.$$

所以需要 $360k(k>0)$ 人.

点评 这是求数个整数的最小公倍数的问题，其手算方法如上. 由于考虑到问题的实际意义，答案应取正整数.

1.4-4 方程 $ax+by=c$ 在整数范围内有解的充分必要条件是 $(a,b)\mid c$.

分析 需要用到最大公因子的性质.

证 必要性：设方程有解，则存在 $m,n\in\mathbb{Z}$ 满足 $am+bn=c$，由于 $(a,b)\mid a$，$(a,b)\mid b$，故 $(a,b)\mid am+bn$，所以 $(a,b)\mid c$.

充分性：设 $d=(a,b)$，$d\mid c$. 由最大公因子定理，存在整数 p,q 使 $pa+qb=d$. 又由 $d\mid c$，可设 $c=dh$. 可得 $pah+qbh=dh=c$. 所以 $x=ph$，$y=qh$ 就

是方程 $ax+by=c$ 的一个解.

点评 证明必要性比较容易.证明充分性主要利用最大公因子定理.问题:有解时是否还有其他的解?如有,求出所有的解.(答案可在本章的某处找到)

1.4-5 分别解同余方程:

(1) $258x=131 \pmod{348}$;

(2) $56x=88 \pmod{96}$.

分析 首先要判断方程是否有解,在有解的情况下,按照书中的步骤来解.

解 (1) 求 $(a,m)=(258,348)=6$,由于 6 不能整除 131,所以此同余方程无解.

(2) 求 $(a,m)=(56,96)=8$,由于 8 能整除 88,所以此同余方程有解.

按照解同余方程的四个步骤:

① 求 $d=8$;

② 求 $a_1=a/d=7, b_1=b/d=11, m_1=m/d=12$;

③ 用辗转相除法求 p,q 使 $pa_1+qm_1=1$,得 $p=-5$;

④ 所以方程的解为 $x\equiv pb_1\equiv 5 \pmod{12}$,或 $x=5+12k$(k 为任意整数).

点评 该题的目的是熟悉同余方程的求解问题,虽然读者从中小学就开始解代数方程的问题,但较少遇到整数解的问题,更少遇到同余方程的问题,而这些概念和算法是学代数的基础,应熟练掌握.

1.4-6 解同余方程组:

$$\begin{cases} x \equiv 3 \pmod{5}, \\ x \equiv 7 \pmod{9}. \end{cases}$$

分析 这是两个方程的同余方程组问题.可用公式(1.4).

解 首先我们应检验一下 m_1, m_2 是否互素.然后按公式(1.4)来做.

观察得到 $2\times 5+(-1)\times 9=1, p=2, q=-1$.所以此同余方程组的解为

$$\begin{aligned} x &\equiv b_1qm_2+b_2pm_1 \pmod{m_1m_2} \\ &= 3\times(-1)\times 9+7\times 2\times 5 \pmod{45} \\ &= 43 \pmod{45}. \end{aligned}$$

点评 两个方程的同余方程组比较简单,公式比一般的孙子定理好记.

1.4-7 韩信点兵:有兵一队,若列成 5 行,则多 1,成 6 行,多 5,成 7 行,多 4,成 11 行,多 10,求兵数.

分析 这是一个应用题,可用同余方程组来解.

解 设兵数为 x,则 x 满足以下同余方程组:

$$\begin{cases} x \equiv 1 \pmod 5, \\ x \equiv 5 \pmod 6, \\ x \equiv 4 \pmod 7, \\ x \equiv 10 \pmod{11}. \end{cases}$$

按解同余方程组的步骤，计算如下：

$M = 5 \times 6 \times 7 \times 11 = 2310, M_1 = 462, M_2 = 385, M_3 = 330, M_4 = 210.$

分别解以下一次同余式：

$$462x = 1 \pmod 5), \quad \text{得} \quad c_1 = 3.$$
$$385x = 1 \pmod 6), \quad \text{得} \quad c_2 = 1.$$
$$330x = 1 \pmod 7), \quad \text{得} \quad c_3 = 1.$$
$$210x = 1 \pmod{11}), \quad \text{得} \quad c_4 = 1.$$

代入同余方程组的解的公式，得

$$\begin{aligned} x &\equiv b_1 c_1 M_1 + b_2 c_2 M_2 + \cdots + b_k c_k M_k \pmod M, \\ &= 1 \times 3 \times 462 + 5 \times 1 \times 385 + 4 \times 1 \times 330 \\ &\quad + 10 \times 1 \times 210 \pmod{2310} \\ &= 2111 \pmod{2310}. \end{aligned}$$

由实际问题的意义，x 应取正数，所以兵数为

$$x = 2111 + 2310k \quad (k \text{ 非负整数}).$$

点评　一般来说孙子定理比较长，不一定记得住，遇到时会查就可.

第 1 章补充题

补充题 1-1　证明 n 维欧氏空间中有且最多有 $n+1$ 个互夹钝角的向量.

分析　这是线性代数的问题，一方面，因为线性代数是学习近世代数的重要基础；另一方面，通过这个题，引起对证明方法的重视，如何用简洁的语言严格证明理论问题.

对于这个问题，首先可以从直观入手，先看一维的情况，显然有两个方向相反的向量，它们夹 180°. 再看二维的情况，显然也有 3 个互夹钝角的向量. 对于三维的情况，我们只要把 xy 平面上的 3 个互夹钝角的向量的原点往 z 轴正方向拉一个很小的距离，则与 z 轴上的向量形成 4 个互夹钝角的向量，如此等等，所以该题可用归纳法来做，按上述方法构造出 $n+1$ 互夹钝角的向量.

证　(1) 先证存在性：对 n 作归纳法. $n=1$ 显然成立.

下设 $n>1$，由归纳假设，$\mathbb{R}^{n-1}$ 中有 n 个互夹钝角的向量，设为

$$\alpha_i = (a_{i1}, a_{i2}, \cdots, a_{in-1}), i = 1, 2, \cdots, n, \quad \text{且} \quad (\alpha_i, \alpha_j) < 0, i \neq j.$$

在 $\mathbb{R}^n$ 中取向量：

$$\beta_i = (a_{i1}, a_{i2}, \cdots, a_{in-1}, b), \quad i = 1,2,\cdots,n,$$
$$\beta_{n+1} = (0,0,\cdots,0,-1).$$

其中实数 b 满足条件：$0<b<\sqrt{\min\limits_{1\leqslant i<j\leqslant n}|(\alpha_i,\alpha_j)|}$.

则有

$$(\beta_i,\beta_j) = (\alpha_i,\alpha_j) + b^2 < 0, \quad 1 \leqslant i < j \leqslant n+1.$$

所以 $\beta_1,\beta_2,\cdots,\beta_{n+1}$ 是$\mathbb{R}^n$中 n 个互夹钝角的向量.

(2) 再证最多有 $n+1$ 个互夹钝角的向量. 对 n 作归纳法. $n=1$ 显然成立.

设 $n>1$，由归纳假设，$\mathbb{R}^{n-1}$中最多有 n 个互夹钝角的向量. 下面用反证法证明$\mathbb{R}^n$中最多有 $n+1$ 个互夹钝角的向量：

假设$\mathbb{R}^n$中有 $n+2$ 个互夹钝角的向量：$\alpha_1,\alpha_2,\cdots,\alpha_{n+2}$.

在 α_{n+2} 的基础上取一组标准正交基：$\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n=\dfrac{\alpha_{n+2}}{|\alpha_{n+2}|}$.

则在这组标准正交基下，$\alpha_1,\alpha_2,\cdots,\alpha_{n+2}$ 的坐标可表示为

$$\alpha_i = (a_{i1}, a_{i2}, \cdots, a_{in-1}, c_i), \quad i = 1,2,\cdots,n+1,$$
$$\alpha_{n+2} = (0,0,\cdots,0,1).$$

由于$(\alpha_i,\alpha_j)<0, i\neq j$ 得 $c_i<0, i=1,2,\cdots,n+1$，和

$$\sum_{k=1}^{n-1} a_{ik}a_{ik} < -c_ic_j < 0, \quad i \neq j.$$

令

$$\gamma_i = (a_{i1}, a_{i2}, \cdots, a_{in-1}), \quad i = 1,2,\cdots,n+1.$$

则

$$(\gamma_i,\gamma_j) < 0, \quad 1 \leqslant i < j \leqslant n+1,$$

得到$\mathbb{R}^{n-1}$中有 $n+1$ 个互夹钝角的向量，与归纳假设矛盾. 证毕.

点评 证明第(1)部分——存在性时，可直接在$\mathbb{R}^n$中构造 $n+1$ 个互夹钝角的向量，例如令

$$\alpha_1 = \left(-1, \frac{1}{n}, \cdots, \frac{1}{n}\right),$$
$$\alpha_2 = \left(\frac{1}{n}, -1, \frac{1}{n}\cdots, \frac{1}{n}\right),$$
$$\vdots$$
$$\alpha_n = \left(\frac{1}{n}, \cdots, \frac{1}{n}, -1\right),$$
$$\alpha_{n+1} = \left(\frac{1}{n}, \frac{1}{n}, \cdots, \frac{1}{n}\right),$$

则有

$$(\alpha_i,\alpha_j)=-\frac{2}{n}+\frac{n-2}{n^2}<0,\quad 1\leqslant i<j\leqslant n,$$

$$(\alpha_i,\alpha_{n+1})=-\frac{1}{n}+\frac{n-1}{n^2}=\frac{-1}{n^2}<0,\quad i=1,2,\cdots,n.$$

所以它们互夹钝角.

该题的内容完全是复习线性代数,同时为了训练证明方法,证明方法是学习这门课的基础.在证明过程中要注意逻辑的严密,语言的简洁,表达的确切.

1.4-4 的点评中所提问题的答案:若 $ax+by=c$ 在整数范围内有解,求所有的解.

解 由习题 1.4-4,得到 $(a,b)\mid c$.令 $d=(a,b)$,$a=da_1$,$b=db_1$.设 x_0,y_0 是 $ax+by=c$ 的一组解,则有

$$ax_0+by_0=c.$$

设 x,y 是 $ax+by=c$ 的任一组解,则有

$$ax+by=c,$$

两式相减,得

$$a(x-x_0)+b(y-y_0)=0\Rightarrow a_1(x-x_0)+b_1(y-y_0)=0$$
$$\Rightarrow b_1\mid(x-x_0),\quad a_1\mid(y-y_0),$$

可设 $x=x_0+rb_1$,$y=y_0+sa_1$,代入原方程可得 $s=-r$.所以 $ax+by=c$ 得全部解为

$$\begin{cases}x=x_0+rb_1,\\ y=y_0-ra_1,\end{cases}\quad r\in\mathbb{Z}.$$

补充题 1-2 证明三维空间中只有 5 种正多面体.

分析 该题要用到欧拉多面体定理:点数−边数+面数=2.

证 设正多面体的面数为 n,每面为正 m 边形($m\geqslant3$),每个顶点与 k 条边(或称棱)相接($k\geqslant3$).

(1) 我们来建立它们的关系.

由于每条边是 2 个面的边界,所以正多面体的边数为 $\frac{mn}{2}$.

又由于顶点数 $\times k=2\times$ 边数,得顶点数为 $\frac{mn}{k}$.

由多面体欧拉定理:顶点数−边数+面数=2 得到方程:

$$\frac{mn}{k}-\frac{mn}{2}+n=2,$$

得

$$n=\frac{4k}{2k+2m-km}.$$

(2) 求整数解：

$m=3$ 时，$n=\frac{4k}{6-k}$，得

$$k=3,\quad n=4;$$
$$k=4,\quad n=8;$$
$$k=5,\quad n=20.$$

$m=4$ 时，$n=\frac{4k}{8-2k}$，得

$$k=3,\quad n=6.$$

$m=5$ 时，$n=\frac{4k}{10-3k}$，得

$$k=3,\quad n=12.$$

所以共有五种情况：正 4,6,8,12,20 面体.

点评　这是一个关系式的整数解的问题. 在近世代数中我们经常要在某个特定范围内的数集中讨论问题，这与微积分有很大的不同，在微积分中我们总是假定在实数范围内讨论问题.

能否将上述讨论更简化一点？

补充题 1-3　证明与所有实 n 阶矩阵可交换的矩阵是数量矩阵.

分析　该题是线性代数中的一个习题，如果没有做过，可做一下，在以后的内容中要用到这个结论.

首先我们反过来看一下，数量矩阵确实与任何矩阵都可交换. 为了证明与任何矩阵都可交换的矩阵必为数量矩阵，设 $A=(a_{ij})$ 与任何矩阵都可交换，只需证明当 $i\neq j$ 时 $a_{ij}=0$，并且 $a_{11}=a_{22}=\cdots=a_{nn}$.

为此，利用矩阵 E_{kl}：第(k,l)个元素是 1，其余元素均为 0. 即

$$E_{kl}=(e_{ij}),e_{ij}=\begin{cases}1, & (i,j)=(k,l),\\ 0, & (i,j)\neq(k,l).\end{cases}$$

证　设 $A=(a_{ij})$ 与任何矩阵都可交换. 取 $E_{kl}(k\neq l)$，A 与 E_{kl} 可交换，由 $AE_{kl}=E_{kl}A$（仔细计算！）可得

$$a_{ik}=0 \text{ 当 } i\neq k,\quad a_{lj}=0 \text{ 当 } j\neq l,\quad a_{kk}=a_{ll}.$$

由于 k,l 可任取，于是得 A 是对角矩阵：$A=\mathrm{diag}\{a_{11},a_{22},\cdots,a_{nn}\}$，且对角元素相等，设

$$a_{11}=a_{22}=\cdots=a_{nn}=\alpha.$$

所以 $A=\alpha I$，是数量矩阵.

点评　怎么会想到利用矩阵 E_{kl}？是否可利用其他的特殊矩阵来做？

补充题 1-4 用最小公倍数的定义证明$(a,b)\cdot[a,b]=ab$.

分析 这里涉及最小公倍数$[a,b]$的定义：设$a,b\in\mathbb{Z}^*$，若有$m\in\mathbb{Z}^*$满足

(1) $a|m$ 和 $b|m$(m 是 a 和 b 的公倍数)；

(2) 若有 $c\in\mathbb{Z}^*$ 满足 $a|c$ 和 $b|c$，则 $m|c$(m 的最小性).

则称 m 是 a 和 b 的最小公倍数. m 和 $-m$ 都是最小公倍数，把正的最小公倍数记作$[a,b]$.

证 令 $d=(a,b)$，并设 $a=a_1d, b=b_1d$，则$(a_1,b_1)=1$.

再令 $x=\dfrac{ab}{d}$，下证：$x=[a,b]$.

(1) 由于 $x=ab_1=a_1b$，所以 $a|x$ 和 $b|x$.

(2) 如有 y 满足：$a|y$ 和 $b|y$，可设 $y=ah=a_1dh$，$y=bk=b_1dk$，得 $a_1h=b_1k$.

由互素性质(3)，有 $b_1|h$，因而可设 $h=b_1h_1$. 于是得到

$$y=a_1dh=a_1db_1h_1=ab_1h_1,$$

所以 $x|y$.

综上，$x=[a,b]$，因而公式成立.

点评 这个证明比用整数的素因子分解式来证要复杂一些.

补充题 1-5 证明以下性质：

(1) $(a,b)=1\Leftrightarrow\exists\, p,q\in\mathbb{Z}$ 使 $pa+qb=1$；

(2) $a|bc$ 且$(a,b)=1\Rightarrow a|c$；

(3) 设 p 为素数，则有 $p|ab\Rightarrow p|a$ 或 $p|b$；

(4) $(a,b)=1$ 且$(a,c)=1\Rightarrow(a,bc)=1$；

(5) $a|c, b|c$ 且$(a,b)=1\Rightarrow ab|c$.

分析 证明的出发点主要是最大公因子定理.

证 (1) 主要证明充分性：设$\exists\, p,q\in\mathbb{Z}: pa+qb=1$，由于$(a,b)|(pa+qb)\Rightarrow(a,b)|1$，所以$(a,b)=1$.

(2) $a|bc$ 且$(a,b)=1\Rightarrow\exists\, p,q\in\mathbb{Z}: pa+qb=1\Rightarrow pac+qbc=c$，由于 $a|(pac+pbc)$，所以 $a|c$.

(3) 设 p 为素数，$p|ab$，若 $p\nmid a$，则$(p,a)=1$，由性质(2)得 $p|b$.

(4) $(a,b)=1$ 且$(a,c)=1\Rightarrow pa+qb=1, ra+sc=1\Rightarrow(pra+psc+qrb)a+qsbc=1\Rightarrow(a,bc)=1$.

(5) $a|c, b|c$ 且$(a,b)=1\Rightarrow pa+qb=1\Rightarrow pac+qbc=c\Rightarrow ab|(pac+pbc)$，所以 $ab|c$.

点评 性质(1)能否推广到一般：$(a,b)=d\Leftrightarrow\exists\, p,q\in\mathbb{Z}: pa+qb=d$?

补充题 1-6 设$(m,k)=1$,证明 $\varphi(mk)=\varphi(m)\varphi(k)$. 并由此证明欧拉函数公式.

分析 如果从 $\varphi(n)$的公式出发,证明非常简单. 现要求先于 $\varphi(n)$的公式证明此式.

证 令 $n=mk$, $X=\{x|x\in[1,n],(x,n)=1\}$, $A=\{a|a\in[1,m],(a,m)=1\}$, $B=\{b|b\in[1,k],(b,k)=1\}$. 作映射:
$f:x\mapsto(a(x),b(x))(X\to A\times B)$,其中 $a(x)=x(\text{mod } m)$, $b(x)=x(\text{mod } k)$. 先证 f 是单射: $a(x_1)=a(x_2)$, $b(x_1)=b(x_2)\Rightarrow x_1(\text{mod } m)=x_2(\text{mod } m)$, $x_1(\text{mod } k)=x_2(\text{mod } k)\Rightarrow m|(x_1-x_2)$, $k|(x_1-x_2)\Rightarrow n|(x_1-x_2)\Rightarrow x_1=x_2$.

再证 f 是满射: 任取$(a,b)\in A\times B$,令 $x\equiv a(\text{mod } m)$, $x\equiv b(\text{mod } k)$,得到一个同余方程组. 由孙子定理,有解 x,且在 1 到 n 的范围内解是惟一的.

综上,f 是双射,故有$|X|=|A\times B|$,即 $\varphi(mk)=\varphi(m)\varphi(k)$. 证毕.

下面利用此公式证明欧拉函数公式.

设 $n=p_1^{r_1}\cdots p_s^{r_s}$ 为 n 的标准分解式.

对 s 作归纳法. $s=1$, $n=p_1^{r_1}$,由于$[1,p_1^{r_1}]$中可被 p_1 整除的整数个数为 $\frac{p_1^{r_1}}{p_1}=p_1^{r_1-1}$,所以有 $\varphi(n)=p_1^{r_1}-p_1^{r_1-1}=n\left(1-\frac{1}{p_1}\right)$.

下设 $s>1$,且欧拉公式对 $s-1$ 成立. 把 n 表示为 $n=(p_1^{r_1}\cdots p_{s-1}^{r_{s-1}-1})p_s^{r_s}=mk$,则$(m,k)=1$,由 $\varphi(mk)=\varphi(m)\varphi(k)$和归纳假设得

$$
\begin{aligned}
\varphi(n)&=\varphi(mk)=\varphi(m)\varphi(k)\\
&=m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_{r_{s-1}}}\right)k\left(1-\frac{1}{p_{r_s}}\right)\\
&=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_{r_s}}\right).
\end{aligned}
$$

点评 这个证明包含了孙子定理的一个很好的应用,值得回味. 同时给出了欧拉 φ 函数的另一个证明方法.

注 当 p 不能整除 a 时,记作 $p\nmid a$ 或 $p\rceil a$。但由于记号 $p\rceil a$ 在本文中另有用处,所以不要标混。

第2章　群　　论

群论是本书的重点，其他的代数系均以群为基础，学好了群论，再学环论和域论等就可举一反三．所以学群论时要多琢磨，多问几个为什么．习题要细致地做．

2.1　群的基本概念

一、内容提要

这一节的内容是整个近世代数的基础，必须慢慢入门，学得扎实．我们在学习微积分时，满脑子是曲线．可是学习近世代数时，我们应该换成满脑子是一些点（元素），这些点互相有关联，例如两点之间进行运算后变成另外一个点等．整个集合有许多奇特的结构和性质．我们就是要研究不同的集合所具有的独特的结构和性质．

1. 群（与半群）的定义

定义 2.1.1　非空集合上定义一个二元运算满足结合律，就是一个半群；如果还满足：有单位元，并且每一个元素有逆元，则称它是一个群．

为了便于记忆，简单地说，集合对运算满足：封闭性，结合律，有单位元和有逆元，就称为一个群．

2. 群的几个等价的定义

（1）半群有左单位元和左逆元是群．

（2）半群满足：方程 $ax=b$ 和 $xa=b$ 有解，则是群．

（3）有限半群满足左、右消去律是群．

3. 几个重要的例

这些例非常重要！手中有典型，学抽象理论时有背景，就容易理解．

（1）**数群**：$(\mathbb{Z},+)$，$(\mathbb{Q},+)$，$(\mathbb{R},+)$，$(\mathbb{C},+)$，$(\mathbb{Q}^*,\cdot)$，$(\mathbb{R}^*,\cdot)$，$(\mathbb{C}^*,\cdot)$等．

数半群：$(\mathbb{Z},\cdot)$，$(\mathbb{Q},\cdot)$，$(\mathbb{R},\cdot)$，$(\mathbb{C},\cdot)$等．

(2) **Klein 四元群**:

$$K_4 = \{e, a, b, c \mid a^2 = b^2 = c^2 = e, ab = ba = c,$$
$$ac = ca = b, bc = cb = a\}.$$

(3) **整数模 n 的同余类群和半群**:

- **整数模 n 的加法群**:$(\boldsymbol{Z}_n,+)$. 这个群的重要性再怎么强调也不过分,是五星级的.

特别是对于搞数字通信的工程人员来说,学懂了群$(Z_n,+)$和以后的环$(Z_n,+,\cdot)$和域$(Z_p,+,\cdot)$是至关重要的.

群$(Z_n,+)$的定义有两种形式:

定义 A 设 $Z_n=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$,加法运算为模 n 的加法:$\bar{a}+\bar{b}=\overline{a+b}$.(注意左边的加号与右边的加号意义不同,理应用不同的记号,但为了简单,通常心照不宣,心里知道就行.)

定义 B 设 $Z_n=\{0,1,\cdots,n-1\}$,其中的每一个元素代表的是以它为代表的同余类,加法运算为取模 n 的余数:$a+b=(a+b) \bmod n$. 也即总是用同余类的正则代表元表示该同余类. 这种表示方法书写简单,但概念上不要与一个数混淆,例如 $Z_6=\{0,1,\cdots,5\}$,$3+4=(3+4) \bmod 6=1$,对应定义 1 中的同余类的加法:$\bar{3}+\bar{4}=\bar{1}$.

用定义 B 是为了书写简单,对其元素仍应理解为模 n 的同余类.

- **整数模 n 的同余类乘法半群**:$(Z_n,\cdot)$.
- **整数模 n 的同余类乘法群**:$(Z_n^*,\cdot)$,其中 $Z_n^*=\{\bar{k}\in Z_n \mid (k,n)=1\}$. $|Z_n^*|=\varphi(n)$.

(4) **矩阵群:全矩阵加法群$(\boldsymbol{M}_n(\boldsymbol{F}),+)$;全矩阵乘法半群$(\boldsymbol{M}_n(\boldsymbol{F}),\cdot)$;全线性群$(\boldsymbol{GL}_n(\boldsymbol{F}),\cdot)$**,指全体可逆阵的乘法群.

(5) **置换群,n 次对称群**:

有限集上的可逆变换所构成的群称置换群,n 元集合上的全体置换所构成的群称为 n 次对称群. 对置换群我们以后要专门讨论.

(6) **二面体群 $\boldsymbol{D}_n$**:

- 几何定义:正 n 边形的旋转群为 $D_n=\{\rho_k,\pi_k \mid k=0,1,\cdots,n-1\}$,$\rho_k\rho_l=\rho_{k+l}$,$\rho_k\pi_l=\pi_{k+l}$,$\pi_k\rho_l=\pi_{k-l}$,$\pi_k\pi_l=\rho_{k-l}$. 其中脚标的加法为模 n 取余数的加法.

几何定义比较直观,很容易记忆. 但元素之间的运算关系需要找出规律才能记忆,初学时不妨用到时查一下. 有些东西通过不断查阅就记住了.

- 代数定义:以后再说,见习题 2.3-1.

4. 群中元素的运算符号

对抽象的群,其中的运算一般用乘号表示,因而按惯例可省略.逆元与幂的运算满足通常的规律:$a^m a^n = a^{m+n}$,$(a^m)^n = a^{mn}$,$(ab)^{-1} = b^{-1}a^{-1}$等,不一一列举了.

交换群又称 Abel 群,加群.运算符有时可用加号表示:$(G,+)$,这时称为加群.在加群中,与乘号群中的单位元对应的是 0 元;与乘号群中的逆元对应的是负元:$-a$;与乘号群中的幂元对应的是倍元:na.但对于具体的群,其运算符号按惯例,是不能随便更改的.例如群$(\mathbb{Q}^*,\cdot)$,它是普通乘法,虽是可换群,但不能用加号表示.又如$(Z_n,+)$,$(Z_n,\cdot)$,$(Z_n^*,\cdot)$等,运算符是规定的.

二、习题 2.1 详细解答

2.1-1 设 $G=\{A=(a_{ij})_{n\times n} \mid a_{ij}\in\mathbb{Z}, \det A=1\}$,证明 G 对矩阵乘法构成群.

分析 作为初学者必须严格按定义逐条检验.

证 封闭性:$\forall A,B\in G$,$\det(AB)=(\det A)(\det B)=1$,所以 $AB\in G$.

结合律:矩阵乘法满足结合律.

单位元:单位矩阵 I 的行列式$|I|=1$,所以 $I\in G$.

逆元:$\forall A\in G$,$|A|\neq 0$,故 A 可逆,且因 $A^{-1}=\dfrac{1}{\det A}A^*=A^*$,故 A^{-1}的元素仍为整数,且$|A^{-1}|=|A|^{-1}=1$,所以 $A^{-1}\in G$.

综上,G 对矩阵乘法构成群.

点评 这是概念题,对初学者来说,必须按定义条件逐一检验.此外,此题看起来简单,实际上,也有不是很显然的地方.例如,逆元的问题,一般,一个整数元素的可逆矩阵,其元素不一定仍是整数,而该题由于行列式为 1,所以逆矩阵里的元素仍为整数.

该题可推广到以下集合:$H=\{A=(a_{ij})_{n\times n} \mid a_{ij}\in\mathbb{Z}, |A|=\pm 1\}$,对矩阵乘法构成群.

2.1-2 设 $Q_8=\{\pm E,\pm I,\pm J,\pm K\}$,其中

$$E=\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad I=\begin{bmatrix}0&-1\\1&0\end{bmatrix},\quad J=\begin{bmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{bmatrix},\quad K=\begin{bmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{bmatrix},$$

$\mathrm{i}^2=-1$.

证明 Q_8 对矩阵乘法构成群.

分析 这是一个有限群,要证明封闭性,一般来说要计算一个乘法表,看看每个乘积是否仍在集合里.对本题需要计算如一个 8×8 的乘法表,很麻烦.

所以应找一下规律,将其表达得简单一些.

证 我们不妨先看出单位元: E.

封闭性: $I^2=J^2=K^2=-E$, $IJ=K=-JI$, $JK=I=-KJ$, $KI=J=-IK$.

结合律: 矩阵乘法满足结合律.

逆元: $E^{-1}=E, I^{-1}=-I, J^{-1}=-J, K^{-1}=-K$.

综上, Q_8 对矩阵乘法构成群.

点评 (1) 该题的主要之点是证明封闭性,一般来说,对于有限集合应列一个乘法表,看乘积是否仍在原集合中.

(2) 这是一个非常重要的群: 8 阶非可换群,称为**四元数群**,以后会用到它,最好记住它的名字,以后用到时可到这里来查它的定义.

2.1-3 设 $G=\left\{f(x)=\frac{ax+b}{cx+d}\,\middle|\,a,b,c,d\in\mathbb{R},\ \begin{vmatrix}a & b\\ c & d\end{vmatrix}=1\right\}$,证明 G 关于变换的复合构成群.

分析 继续熟悉群的定义,同时对群的种类扩大范围.

证 封闭性: 任取 $f_1,f_2\in G$,设 $f_1(x)=\frac{a_1x+b_1}{cx+d_1}$, $f_2(x)=\frac{a_2x+b_2}{c_2x+d_2}$,令 $f_3(x)=\frac{a_3x+b_3}{c_3x+d_3}=f_1(f_2(x))$,经过计算,得到

$$\begin{bmatrix}a_3 & b_3\\ c_3 & d_3\end{bmatrix}=\begin{bmatrix}a_1 & b_1\\ c_1 & d_1\end{bmatrix}\begin{bmatrix}a_2 & b_2\\ c_2 & d_2\end{bmatrix},$$

由于

$$\det\begin{bmatrix}a_3 & b_3\\ c_3 & d_3\end{bmatrix}=\det\begin{bmatrix}a_1 & b_1\\ c_1 & d_1\end{bmatrix}\cdot\det\begin{bmatrix}a_2 & b_2\\ c_2 & d_2\end{bmatrix}=1,$$

所以 $f_3=f_1f_2\in G$,封闭性成立.

结合律: 集合上的变换满足结合律.

单位元: $e(x)=x=\frac{1\cdot x+0}{0\cdot x+1}\in G$.

逆元: 任取 $f(x)=\frac{ax+b}{cx+d}\in G$,设 $f^{-1}(x)=\frac{a'x+b'}{c'x+d'}$,其中 $\begin{bmatrix}a' & b'\\ c' & d'\end{bmatrix}=\begin{bmatrix}a & b\\ c & d\end{bmatrix}^{-1}$. 显然 $f^{-1}\in G$.

综上, G 对变换的复合构成群.

分析 这是一个变换群的例子,但可转化为矩阵群来分析. 以后我们在学

习了群的同构以后，就知道这个群与一个行列式为1的二阶实线性群同构.

2.1-4 举例说明，把定理2.1.3(半群$(G,\cdot)$是群的充要条件.是满足两个条件：(1)S_2'：G中有左单位元e_L：对任何$a\in G$有$e_La=a$；(2) S_3'：对任何$a\in G$有以下形式的左逆元a^{-1}：$a^{-1}a=e_L$.)中条件S_3'改为

对任意a有右逆元a_R^{-1}：$aa_R^{-1}=e_L$，则定理不成立.

分析 首先我们应复习一下教材上的定理2.1.3，然后把它改为以下命题：半群$(G,\cdot)$是群的充分必要条件是：

S_2'：G中存在左单位元e_L：$\forall a\in G$有$e_La=a$；

S_3'：$\forall a\in G$存在右逆元a_R^{-1}：有$aa_R^{-1}=e_L$.

要证明该命题不成立，应举一个反例.显然，应举一个不可交换的半群的例子.具体方法可在已有的例子中找，或构造一个例子.

证 方法1 构造一个抽象的半群.

设$G=\{a,b\}$，乘法表如下：

$\times$	a	b
a	a	b
b	a	b

可验证满足结合律，故$(G,\times)$是半群.

左单位元为a.

右逆元：$a_R^{-1}=a$，$b_R^{-1}=a$.

但a和b都不是单位元，所以G不是群.因此修改后的命题不成立.

方法2 由于矩阵乘法半群$M_n(F)$(例2.1.7)与置换群(例2.1.8)是不可交换的，我们可以从它们那里找一个例子，但由于我们对置换群还不太熟悉，而对矩阵的运算非常拿手，所以可从$M_2(\mathbb{R})$中找一个例子.设$G=\{a,b\}$，其中

$$a=\begin{bmatrix}1&0\\0&0\end{bmatrix},\quad b=\begin{bmatrix}1&1\\0&0\end{bmatrix}.$$

由于$a^2=a$，$ab=b$，$ba=a$，$b^2=b$，所以G对矩阵乘法构成半群.a是左单位元.a的右逆元是a，b的右逆元也是a.但a和b都不是单位元，所以G不是群.因此修改后的命题不成立.

点评 请读者自己举个其他的例子.通过这个习题，进一步熟悉群和半群的概念.学习近世代数的特点是多思考，多提问.做一个题要联想到很多概念，涉及许多例子，甚至留下一些悬念.例如，对于这个题，能否举一个有三个矩阵

的半群的例子？可能不是很容易，如果时间不多的话，可以暂时放一放，等以后有空了再想.

2.1-5 M 为含幺半群，e 是单位元，证明 $b=a^{-1}$ 的充分必要条件是 $aba=a$ 和 $ab^2a=e$.

分析 与初等代数类似，可以对半群和群中的一个代数式进行同乘一个元素的运算. 但由于交换律不一定成立，只能两边同时左乘或右乘同一个元素. 又由于对半群逆元不一定存在，所以在半群中不能随便两边消去同一个元素.

证 必要性：将 b 代入即可得，略.

充分性：要证 $ab=ba=e$. 利用结合律作以下运算：

$$ab = abe = ab(ab^2a) = (aba)b^2a = ab^2a = e,$$

$$ba = eba = (ab^2a)ba = ab^2(aba) = ab^2a = e.$$

所以 $b=a^{-1}$.

点评 在半群或群中有一类题，要进行元素的代数运算，可利用增加一个单位元，左乘在前面，或右乘在后面，或插在中间；也可利用结合律、消去律、逆元等性质.

2.1-6 写出 S_3 的乘法表.

分析 首先把 S_3 的元素写出来，然后算出乘法表. 注意如何计算两个置换的乘积.

解 写出 S_3 的元素：

$$\sigma_1 = e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

作以下乘法表：

$\sigma_i \cdot \sigma_j$	$\sigma_1=e$	σ_2	σ_3	σ_4	σ_5	σ_6
$\sigma_1=e$	e	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	e	σ_5	σ_6	σ_3	σ_4
σ_3	σ_3	σ_6	e	σ_5	σ_4	σ_2
σ_4	σ_4	σ_5	σ_6	e	σ_2	σ_3
σ_5	σ_5	σ_4	σ_2	σ_3	σ_6	e
σ_6	σ_6	σ_3	σ_4	σ_2	e	σ_5

分析 填出上表所需的计算量相当大，其原因是一方面由于元素的表达

形式比较笨拙,打草稿时需要很大的书写工作量;另一方面,由于此群不可交换,乘法表无对称性,因而不能节省计算.为了解决元素的表达形式比较笨拙的问题,我们在以后将专门讨论如何简化的问题.

2.1-7　设 G 为有限集,用乘法表定义了一个二元运算,且 G 有单位元 1,则 G 是群的充分必要条件是乘法表具有以下性质:

(1) 乘法表中每行与每列都包含 G 的所有元素.

(2) 对 G 中任意两个元素 $x\neq 1, y\neq 1$,在乘法表中任意选取一个 1,设 R 是以 $1,x,y$ 为顶点的长方形,其中 $1,x$ 位于同一列,$1,y$ 位于同一行,则 R 的第四个顶点上的元素只依赖于 x,y,而与 1 的位置选择无关.

分析　在近世代数中,在不致混淆的情况下,为简单起见,用一些常用记号来记近世代数中一些量.例如,把单位元 e 简单记作 1,其实并非是数 1;加群中的逆元记作 $-a$,其实不一定与负数有关,等等.

根据题意我们首先应把乘法表抽象地画出来,然后再在表上分析.

证　由于 G 有有限个元素,可设 $G=\{a_1,a_2,\cdots,a_n\}$.可以想象,可作出一个乘法表,表头上面和左边为这 n 个元素:$a_1,a_2,\cdots,a_n$,中间元素为左边的元素乘上面的元素之积.

必要性:设 G 是群.

(1) 由乘法表的规律,设第 i 行左边的元素为 a,则这一行中间的元素为:$aa_1,aa_2,\cdots,aa_n$.由 $aa_1=aa_2$ 和消去律,得 $a_1=a_2$,矛盾.因而 $aa_1\neq aa_2$.所以第 i 行的元素互不相同.从而有 $\{aa_1,aa_2,\cdots,aa_n\}=G$,即第 i 行包含 G 的每一个元素.类似地,任一列也包含所有元素.

(2) 在乘法表中任取一个 1,在同一列中必有一个 x,在同一行中必有一个 y,设第四个顶点的元素为 z,见图 2.1,则有

$$x=ba^{-1},\quad y=ac,\quad z=bc,$$

所以 $z=bc=xy$,与 1 的位置无关.

充分性:由于封闭性已由乘法表保证,我们首先来证满足结合律.

在证明结合律之前,我们由乘法表的性质(1)、(2),对于乘法表中以 $1,x,y,z$ 为顶点的长方形,必有 $z=bc=xy$.下面证明结合律.

结合律:任取 x,y,z 要证 $(xy)z=x(yz)$.

在乘法表中任取一个 1,在同一列中必有一个 x,在同一行中必有一个 y,则以 $1,x,y$ 为顶点的长方形的第四个顶点的元素为 xy.再看在 y 的同一列中必有一个 1,与这个 1 同一行中必有一个 z,见图 2.2,设以 $1,x,yz$ 为顶点的长方形的第四个顶点的元素为 w,我们来看元素 w 的值:对以 $1,x,yz,w$ 为顶点的长方形,有 $w=x(yz)$.对以 $1,xy,z,w$ 为顶点的长方形,有 $w=$

$(xy)z$. 所以$(xy)z=x(yz)$,即结合律成立.

单位元：题设.

逆元：由(1)保证.

综上,所以 G 为群.

$\cdot$	$\cdots$	a^{-1}	$\cdots$	c	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
a	$\cdots$	1	$\cdots$	y	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
b	$\cdots$	x	$\cdots$	z	$\cdots$

图　2.1

$\cdot$	$\cdots$	a^{-1}	$\cdots$	c^{-1}	$\cdots$	d	$\cdots$
$\vdots$		$\vdots$		$\vdots$		$\vdots$	
a	$\cdots$	1	$\cdots$	y	$\cdots$	yz	$\cdots$
$\vdots$		$\vdots$		$\vdots$		$\vdots$	
b	$\cdots$	x	$\cdots$	xy	$\cdots$	w	$\cdots$
$\vdots$		$\vdots$		$\vdots$		$\vdots$	
c	$\cdots$		$\cdots$	1	$\cdots$	z	$\cdots$

图　2.2

点评　该题告诉我们,如果要检验一个有限半群是否是群可通过它的乘法表来判断,特别是检验结合律,可用题中的(2). 但当元素较多时,工作量也不小.

2.2　子　　群

一、内容提要

注　对抽象的群,我们总是用乘号表示其中的运算,因而通常省略。

1. 子群概念

群 G 中非空子集 H 自己成群,就称 H 是 G 的子群,记作 $H\leqslant G$. 真包含的子群记作 $H<G$. 注意,我们用不等号表示子群关系,与一般的包含关系相区别. G 中的单位子群$\{e\}$和 G 本身称为平凡子群. 单位子群$\{e\}$有时也简记为 1,所以 1 到底是数,还是单位元,或是单位子群,要看具体情况.

2. 非空子集是子群的条件

设 H 是群 G 中的非空子集,则

$$H\leqslant G \Leftrightarrow \forall a,b\in H \text{ 有 } ab^{-1}\in H(\text{或 } a^{-1}b\in H).$$

对有限集往往条件可以放松一点,群 G 中有限子集是子群的充分必要条件是封闭性成立. 即若 H 是群 G 中的有限子集,则 $H\leqslant G\Leftrightarrow \forall a,b\in H$ 有 $ab\in H$.

3. 子群的运算

$H_1,H_2\leqslant G$,则

(1) $H_1 \cap H_2 \leqslant G$.

(2) $H_1 \cup H_2 \leqslant G \Leftrightarrow H_1 \subseteq H_2$ 或 $H_1 \supseteq H_2$.

(3) $H_1 H_2 \leqslant G \Leftrightarrow H_1 H_2 = H_2 H_1$.

注意：一般来说，两个集合的交将保留它们的共同性质，而并就不一定了，而两个子群的并只有一个包含另一个才是子群.

4. 子群的例子

从 2.1 节的例子中可以分别找出许多子群，例如

- $(\mathbb{Z}, +)$中的全部子群为：$H_m = \{km \mid k \in \mathbb{Z}\}$，$m \geqslant 0$ 的整数.
- $(Z_n, +)$中的全部子群为：$N_m = \{k\bar{m} \mid k \in \mathbb{Z}\}$，$m = 0$，$0 < m < n$ 且 $m \mid n$.
- $GL_n(\mathbb{R})$中有子群序列：

$GL_3(\mathbb{R}) = \{A \in \mathbb{R}^{3\times 3} \mid |A| \neq 0\}$，全体三阶可逆矩阵；

$SL_3^{\pm}(\mathbb{R}) = \{A \in \mathbb{R}^{3\times 3} \mid |A| = \pm 1\}$，全体三阶行列式等于 1 或 -1 的矩阵；

$SL_3(\mathbb{R}) = \{A \in \mathbb{R}^{3\times 3} \mid |A| = 1\}$，全体三阶行列式等于 1 的矩阵；

$O_3(\mathbb{R}) = \{A \in \mathbb{R}^{3\times 3} \mid A^{\mathrm{T}} A = I\}$，全体三阶正交矩阵；

$SO_3 = \{A \in \mathbb{R}^{3\times 3} \mid A^{\mathrm{T}} A = I \,\&\, |A| = 1\}$，全体三阶正交且行列式为 1 的矩阵.

它们的关系有：$SO_3 < SL_3(\mathbb{R}) < SL_3^{\pm}(\mathbb{R}) < GL_3(\mathbb{R})$，$SO_3 < O_3 < SL_3^{\pm}(\mathbb{R}) < GL_3(\mathbb{R})$.

5. 元素的阶

$o(a)$是使 $a^n = e$ 的最小正整数，当不存在这样的正整数时，记 $o(a) = \infty$. 元素的阶有以下性质：

(1) $a^m = e \Leftrightarrow o(a) \mid m$.

(2) $o(a) = m$，$o(b) = n$ 且 $ab = ba$，$(m, n) = 1 \Rightarrow o(ab) = mn$.

(3) 若 $\forall a \in G \backslash \{e\}$ 均有 $o(a) = 2$，则 G 是 Abel 群.

(4) 若 $o(a) = n$，$0 < k < n$，则 $o(a^k) = \dfrac{n}{(k, n)}$.

注意：如果对于加群$(G, +)$，以上公式的形式都要变. 例如，元素的阶 $o(a)$的定义为使 $na = 0$ 的最小正整数. $ma = 0 \Leftrightarrow o(a) \mid m$，等等.

二、习题 2.2 详细解答

2.2-1 举一个半群的例子，它有单位元，但它的一个子半群无单位元，或有不同的单位元.

分析　我们可从最简单的数集考虑起,整数集合对普通乘法是含幺半群,而偶数集合是一个无单位元的子半群,再找一个有限的有不同单位元的子半群.也可在线性群中找.

解　举例如下:

(1) $G=(\mathbb{Z},\cdot)$,整数集合对普通乘法构成半群.设 $S=\{2k\mid k\in\mathbb{Z}\}$,它是 G 的子半群,且无单位元.

(2) 设 $G=(M_2(\mathbb{Z}),\cdot)$,对矩阵乘法是半群,有单位元 $\begin{bmatrix}1&0\\0&1\end{bmatrix}$.

$S=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}1&0\\0&0\end{bmatrix},\begin{bmatrix}0&0\\0&1\end{bmatrix}\right\}$是 G 的子半群,无单位元.

$H=\left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}1&0\\0&0\end{bmatrix}\right\}$是 G 的子半群,有单位元 $\begin{bmatrix}1&0\\0&0\end{bmatrix}$.

点评　读者可再举其他的例子.最简单是在半群$(Z_n,\cdot)$中找相应的例子.

2.2-2　设 H 是 G 的有限子集,证明 $H\leqslant G\Leftrightarrow$对任意 $a,b\in H$ 有 $ab\in H$.

分析　虽然与一般的子群条件 $ab^{-1}\in H$ 只差一点,但从意义上来说,有重要的区别,它实际上是说:**群中有限子集是子群的充分必要条件是满足封闭性.**

要证明此结论,我们应复习一下有关有限群的定理——定理 2.1.5:有限半群是群的充要条件是消去律成立.

证　必要性:显然.

充分性:由于封闭性成立,H 是半群.又因群 G 中消去律成立,故 H 中消去律也成立.由定理 2.1.5,知 H 是群.

点评　虽然证明非常简单,但关键是能否想到利用定理 2.1.5.如果我们从一般的子群条件出发来证明此题:那就首先抓住有限性这个条件,设 $H=\{a_1,a_2,\cdots,a_n\}$.其次,为了证明 $ab^{-1}\in H$,要利用第二个条件:封闭性.我们用 b 来右乘 H,由于封闭性和群中消去律成立,必有 $Hb=\{a_1b,a_2b,\cdots,a_nb\}=H$,必有某一个 $a_ib=a$,因而有 $ab^{-1}=a_i\in H$.以上过程实际上重复了主教材定理 2.1.5 的证明.

2.2-3　找出$(\mathbb{Z},+)$和$(Z_{12},+)$中全部子群.

分析　到目前为止我们还没有讨论如何在一个群中找出所有子群的问题,只能从具体问题出发.虽然我们在内容提要中已经给出了结果,但还需要证明.

解　(1) 我们已经知道$(\mathbb{Z},+)$有子群:$H_m=\{km\mid k\in\mathbb{Z}\}$,$m=0,1,2,\cdots$.那么这些是否是它的全部子群呢?下面我们来证明这一点.

设 H 是$(\mathbb{Z},+)$中的任意一个子群，若是单位子群$\{0\}$，则就是 H_0；若 H 是非单位子群，则有非零元 a，它的负元$-a$ 也在里面，而 a 与$-a$ 总有一个是正数，令 $S=\{x\in H|x>0\}$，则 S 非空，由于正整数集合$\mathbb{Z}^+$是良序集，S 有最小元，设为 h.

进一步可证：$\forall x\in H$ 有 $h|x$. 用反证法：假设$h\nmid x$，则用带余除法得 $x=qh+r,0<r<h$，由于 $r=x-qh\in H$，与 h 是S 中的最小元矛盾. 因而有 $h|x$，所以$H=\{kh|k\in\mathbb{Z}\}=H_h$.

综上，我们证明了$(\mathbb{Z},+)$的全部子群为

$$H_m=\{km \mid k\in\mathbb{Z}\},\quad m=0,1,2,\cdots.$$

(2) $(Z_{12},+)$是个有限群，我们把它的所有元素都列出来，总有办法找出它的所有子群. 不过我们可从 12 的因子出发来找出它的全部子群：

$$N_0=\{\bar{0}\},\quad N_1=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{11}\}=Z_{12},$$

$$N_2=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\},\quad N_3=\{\bar{0},\bar{3},\bar{6},\bar{9},\},$$

$$N_4=\{\bar{0},\bar{4},\bar{8},\},\quad N_6=\{\bar{0},\bar{6}\}.$$

但是为什么没有其他的子群？还需要证明：$(Z_{12},+)$的全部子群为 $N_m=\{k\bar{m}|k\in\mathbb{Z}\}$，其中$m=0$ 或 $m|12$. 这样还不如证明更一般的结论：

$(Z_n,+)$的全部子群为 $N_m=\{k\bar{m}|k\in\mathbb{Z}\}$，其中 $m=0$，或 $0<m<n$ 且 $m|n$.

证明方法与(1)类似：

设 N 是$(Z_n,+)$中的任意一个子群，若是单位子群$\{\bar{0}\}$，则就是 N_0；若 N 是非单位子群，每一个元素 $\bar{k}\in N$ 取它的正则表示，即 $0\leqslant k<n$. 令 $S=\{x|\bar{x}\in N,0<x<n\}$，则 S 非空，由于正整数集合$\mathbb{Z}^+$是良序集，S 有最小元，设为 h.

进一步可证：$\forall\bar{x}\in N$ 有 $h|x$ 反证法：假设$h\nmid x$，则用带余除法得 $x=qh+r,0<r<h$，由于$r=x-qh$，$r\in S$，与 h 是 S 中的最小元矛盾. 因而得 $N=\{k\bar{h}|k\in\mathbb{Z}\}=N_h$.

综上，我们证明了$(Z_n,+)$的全部子群为

$N_m=\{k\bar{m}|k\in\mathbb{Z}\}$，$m=0$，或 $0<m<n$ 且 $m|n$.

点评 做此题容易产生的问题是，只列出结果，而没有证明为什么这是全部子群. 另外我们再提一个问题：求群$(Z_n,+)$中子群的个数. 答案可在本节中找到.

2.2-4 设 G 是群，证明对任意 a,b 有 $o(ab)=o(ba)$.

分析 首先简化一下符号，令 $o(ab)=n$，$o(ba)=m$. 然后利用阶的性质，证明 n 与 m 互相整除即可.

证 令 $o(ab)=n$，$o(ba)=m$，由于 $(ab)^n=abab\cdots ab=a(ba)^{n-1}b$，因而由 $o(ab)=n$ 得 $a(ba)^{n-1}b=e$.

$(ab)^n=e\Rightarrow a(ba)^{n-1}b=e\Rightarrow(ba)^n b=b\Rightarrow(ba)^n=e.$

所以有 $m|n$.

类似可得 $n|m$.

综上，得 $n=m$.

点评 此题的关键是把 $(ab)^n$ 展开并变换成 $(ba)^n$.

2.2-5 设 G 是偶数阶群，证明 G 中存在二阶元.

分析 关于二阶元的问题在本节的 2(3) 中已讨论过，我们小结一下：

(1) $o(a)=2\Leftrightarrow a^{-1}=a$.

(2) $o(a)>2\Leftrightarrow a^{-1}\neq a$.

由(2)可知凡是阶数大于 2 的元素与它的逆元不同，这样我们可以把阶数大于 2 的元素与它的逆元配对，剩下的元素只有一阶元和二阶元.

证 设 $|G|=2n$. 利用任何元素 a 与它的逆元的关系：对任何非单位元 a 有：$o(a)>2\Leftrightarrow a^{-1}\neq a$，且 $o(a^{-1})=o(a)>2$. 因而阶数大于 2 的元素总是成对出现的，即阶数大于 2 的元素的个数是偶数. 而 $|G|=2n$，也是偶数，所以，除单位元之外至少有 1 个二阶元.

点评 以上的证明好像不大数学化，是否可以改变一下叙述方式使之更加数学一些？

2.2-6 设 G 是群，对任何 $a,b\in G$ 有 $(ab)^2=a^2b^2$，证明 G 是 Abel 群.

分析 这也是元素的代数运算题，只要把平方的意义写出来就一目了然了.

证 利用群内元素的运算关系.

把 $(ab)^2=a^2b^2$ 写成 $abab=aabb$，由消去律（注意：消去律对任何群都成立）得 $ba=ab$.

所以 G 是 Abel 群.

点评 消去律对任何群都成立. 在群中进行元素的代数运算更加自由，可进行左、右消去律.

2.2-7 设 G 是非 Abel 群，证明 G 中存在非单位元 a,b，且 $a\neq b$ 使 $ab=ba$.

分析 首先可想到一个元素与它的逆元是可交换的，但元素与它的逆元不一定不同，这就与前面讨论的二阶元有关，因为 $a=a^{-1}\Leftrightarrow o(a)\leqslant 2$，所以只有非二阶元，与它的逆元不等，因此只要证明 G 中有阶大于 2 的元素就可以

了.另一个思路是一个元素与它的幂是可交换的,当然要求它们不同,也得到此元素的阶要大于2.

证 利用元素和它的逆可交换,或元素和它的幂可交换.但要求元素和它的逆或幂不等.

由于G是非Abel群,必有阶数大于2的元素a: $o(a)>2$,因而$a^{-1}\neq a$,取$b=a^{-1}$,则有$ab=ba$.

点评 也可用幂来做,请读者自己完成.

2.2-8 G是群,$a\in G$,$o(a)=n$,$m\in\mathbb{Z}^+$,证明$o(a^m)=n/(m,n)$.

分析 参看主教材中例2.2.3,令$o(a^m)=r$,$n/(m,n)=s$,要证明它们相等,只要它们互相能整除即可.

证 要证两个整数相等,通常用互相能整除的方法.令

$$o(a^m)=r,\quad n/(m,n)=s.$$

再令$(m,n)=d$,$m=td$,则$n=sd$,$(s,t)=1$.

由$(a^m)^s=a^{\frac{mn}{d}}=(a^n)^t=e$,得$r|s$.

另一方面,由$(a^m)^r=a^{mr}=e$,得$n|mr$.进一步可得

$$n\mid mr\Rightarrow sd\mid tdr\Rightarrow s\mid tr((s,t)=1)\Rightarrow s\mid r.$$

综上,所以$r=s$.证毕.

点评 以上的证明方法在群论里经常用到.(*群$(Z_n,+)$中子群的个数:写出n的标准分解式:$n=p_1^{n_1}\cdots p_s^{n_s}$,则全部子群的个数为$\prod_{i=1}^{s}(n_i+1)$.证明留给大家.)

2.2-9 设$A\in SO_3$,η为旋转变换A的旋转轴的单位向量,θ为按右手法则的旋转角,证明:

(1) η可由$A-I$中两线性无关的行向量作叉积得到;

(2) θ满足$2\cos\theta+1=\mathrm{tr}A$.

分析 SO_3为全体行列式为1的正交矩阵的集合(见主教材中例2.2.2),它的几何意义为三维实线性空间中全体旋转变换.所以每一个$A\in SO_3$代表一个旋转,η为A的旋转轴向量,θ为按右手法则的旋转角,问题是如何由A求出η和θ?这需要较强的线性代数的知识.

证 给定一个A,如何来确定它所对应的旋转轴η和旋转角θ呢?旋转轴η就是三维空间中的一个向量,旋转角θ就是按右手法则转过的角度.设$A\neq I$(如果$A=I$,很易验证结论成立),则向量η确定的方法如下:

(1) 向量η的特点是在A的作用下不变,故满足$A\eta=\eta$,即

$$(A-I)\eta=0.\qquad (*)$$

由于 A 是行列式为 1 的正交矩阵,1 必是 A 的一个特征值(为什么?),所以方程(*)必有非 零解,旋转轴 η 就是特征值 1 所对应的特征向量. 因此如果给出具体的矩阵 A,通过求 A 的特征值和特征向量就可以求出旋转轴 η. 但是对一般的正交矩阵不能通过数字计算的方法来求出旋转轴 η,我们可以给出一个简单的计算方法如下:

首先,由于方程(*)有非零解,得 $\mathrm{r}(A-I)<3$. 但也不可能等于 1,如果秩$(A-I)=1$,则 $\lambda=1$ 的几何重数(即对应的线性无关的特征向量数)为 2,因而 $\lambda=1$ 的代数重数(即特征多项式中因子$(\lambda-1)$的重数)大于或等于 2,则由特征值与行列式的关系 $|A|=\lambda_1\lambda_2\lambda_3$,得 3 个特征值均为 1,因而有 $A=I$,矛盾. 所以

$$\mathrm{r}(A-I)=2.$$

再由方程(*)可见,η 与 $A-I$ 的行向量正交,而 $A-I$ 中恰有两个线性无关的行向量,所以用这两个线性无关的行向量作叉积就得到 η. 于是我们得到计算 η 的方法如下:

在 $A-I$ 中任取两个线性无关的行向量 α,β,则 $\eta=\alpha\times\beta$,并易见 η 是单位向量.

(2) 求旋转角 θ: 设已得到旋转轴向量 η,将 η 扩大为一组标准正交基:$\varepsilon_1=\eta/|\eta|,\varepsilon_2,\varepsilon_3$. 则旋转变换 A 在此组基下的矩阵为

$$B=\begin{bmatrix}1 & 0 & 0\\ 0 & \cos\theta & -\sin\theta\\ 0 & \sin\theta & \cos\theta\end{bmatrix}.$$

由于 A 与 B 相似,它们有相同的迹,所以 $2\cos\theta+1=\mathrm{tr}A$,所以旋转角 θ 满足

$$\cos\theta=\frac{1}{2}(a_{11}+a_{22}+a_{33}-1).$$

点评 此题实际上是一个线性代数的题,与群论没有关系,只是起了对群 SO_3 加深印象的作用.

2.3 循环群和生成群,群的同构

一、内容提要

本节的内容有三,我们不妨改变教材上的次序来叙述.

1. 群的同构

两个群,如果可建立一一对应的关系,且保持运算,则它们同构. 用式子来表达,就是

$G_1 \cong G_2 \Leftrightarrow \exists$ 双射 $f: G_1 \to G_2$ 使 $\forall a, b \in G_1$ 有 $f(ab) = f(a)f(b)$.
有了同构的概念,我们可以把群分类,从而简化对群的讨论.

2. 生成子群与生成元、生成元集

生成子群的定义:$\langle S \rangle$=包含子集 S 的最小子群. 从运算的角度可表述为:若一个子群的所有元素可表示为子集 S 中某个或某些元素的幂(包括**负幂**)的有限乘积(这里的有限,指乘积中的元素个数是有限个,不能是无穷乘积),那么 S 就称为此子群的生成元集. 最小生成元集指元素个数最少. 如果一个群可由一个元素生成,则称为循环群.

生成元集有性质:设 $H \leqslant G, S \subseteq H$,则 $\langle S \rangle \leqslant H$.

3. 循环群

$G=\langle a \rangle$,这是一类最简单而重要的群.

(1) **循环群及其生成元**:循环群只有两类:

无限循环群:$\{a^i \mid o(a)=\infty, i=0, \pm 1, \pm 2, \cdots\} \cong (\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$. 无限循环群的生成元只有 1 或 -1.

有限循环群:n 阶循环群记作 C_n 并与 $(Z_n, +)$ 同构:

$$C_n = \{a^i \mid o(a) = n, i = 0, 1, \cdots, n-1\} \cong (Z_n, +) = \langle \bar{k} \rangle, \quad (k, n) = 1.$$

C_n 中生成元的个数等于 $\varphi(n)$. 由于 Z_n 对不同的运算构成不同的代数系,我们用特殊的记号 C_n 表示循环群 $(Z_n, +)$,即

$$C_n = (Z_n, +).$$

但在有些书上,直接用 Z_n 表示循环群,到环论里又用它表示环,读者在看参考书时要注意区分.

(2) **循环群的子群**:(用生成元的形式表达)

$(\mathbb{Z}, +)$ 的全部子群为:$\langle m \rangle, m=0,1,2,\cdots$. 因而有无限多个子群.

$(Z_n, +)$ 的全部子群为:$\langle \bar{k} \rangle, k=0$,或 $k \mid n$ 且 $0<k<n$. 子群的个数等于 n 的因子数.

二、习题 2.3 详细解答

2.3-1　设 G 是由 a, b 两个元素生成的群,其定义如下:

$$G = \langle a, b \mid o(a) = n, o(b) = 2, ba = a^{-1}b \rangle,$$

写出 G 的所有元素,并证明 $G \cong D_n$. G 也可作为二面体群 D_n 的定义.

分析　首先要复习生成群的意义. G 是由 a, b 两个元素生成的,一般来说两个元素的幂的乘积也是很多的,但可以利用给出的规则加以简化.

证　首先写出 G 的所有元素. 利用 $ba=a^{-1}b$,可把乘积中的 a 的幂换到

前面，于是 G 的任意一个元素都可表示为 a 的幂与 b 的幂，再利用 a,b 的阶，可把 G 表示为

$$G=\{a^ib^j \mid i=0,1,\cdots,n-1;j=0,1\},$$

并得到 $|G|=2n$.

主教材 2.1 节二面体群的几何定义为

$$D_n=\{\rho_k,\pi_k \mid k=0,1,\cdots,n-1\}.$$

为了证明 G 和 D_n 同构，我们把 D_n 的元素改写为与 G 的元素相同的形式：

因为 $\rho_k=\rho_1^k,\pi_k=\rho_k\pi_0=\rho_1^k\pi_0$，所以 D_n 可表示为

$$D_n=\{\rho_1^k\pi_0^l \mid k=0,1,\cdots,n-1;l=0,1\}.$$

然后作映射

$$f:a^ib^j\mapsto\rho_1^i\pi_0^j(G\to D_n),$$

显然是双射，不难证明保持运算（略），所以

$$G\cong D_n.$$

点评 主教材 2.1 节的二面体群 D_n 的定义是几何定义，而现在给出的表达式是二面体群的代数定义. 我们把它们表达如下：

- D_n 的几何定义——正 n 边形的旋转群：

$$D_n=\{\rho_k,\pi_k \mid k=0,1,\cdots,n-1\},$$

$$\rho_k\rho_l=\rho_{k+l},\quad \rho_k\pi_l=\pi_{k+l},\quad \pi_k\rho_l=\pi_{k-l},\quad \pi_k\pi_l=\rho_{k-l}.$$

其中脚标的加法为模 n 的加法，并取正则代表元.

- D_n 代数定义：

$$D_n=\langle a,b \mid o(a)=n,o(b)=2,\quad ba=a^{-1}b\rangle.$$

以后用到二面体群的问题，将根据需要采用不同形式.

2.3-2 求二面体群 D_n 的所有最小生成元集.

分析 最小生成元集指元素个数最少. 因为 D_n 不是循环群，所以 D_n 的最小生成元集中元素的个数必为 2. 由于 D_n 有两种表达方式，虽然代数形式已经是最小生成元集的形式，只需再找其他的最小生成元集. 但我们对几何表达形式比较熟悉，所以我们选择从几何表达形式来分析.

解 由于 D_n 的最小生成元集所含元素个数为 2. 这两个元素不可能是两个旋转 ρ_i,ρ_j，因为它们只能生成循环群. 因而只可能有以下两种情形：

(1) 由一个旋转 ρ_k 和一个翻转 π_l 组成. 我们来看对 k 与 l 有什么条件？根据循环群 $\langle\rho_1\rangle$ 的生成元的性质，得 $(k,n)=1$；而对 l 没有要求，所以这类最小生成元集为

$$D_n=\langle\rho_k,\pi_l\rangle,\quad (k,n)=1,\quad l=0,1,\cdots,n-1.$$

(2) 由两个翻转 π_k,π_l 组成. 我们来看对 k 与 l 有什么条件？由于 $\pi_k\pi_l=$

ρ_{k-l}和必须能生成 n 阶循环群的生成元，因此有$(k-l,n)=1$，所以这类最小生成元集为

$$D_n=\langle \pi_k,\pi_l\rangle,\quad (k-l,n)=1.$$

点评 也可选择 D_n 的代数定义来分析此问题，读者可以自己做一下. 最后我们要问一下，D_n 的最小生成元集的个数是多少？第(1)类的个数很好算，为 $n\varphi(n)$. 第(2)类的个数可形式上表示为：$\sum\limits_{\substack{1\leqslant m<n\\(m,n)=1}} m$. 故全部最小生成元集的个数为

$$n\varphi(n)+\sum_{\substack{1\leqslant m<n\\(m,n)=1}} m.$$

2.3-3 证明 $K_4\cong(Z_{12}^*,\cdot)$.

分析 首先应复习 K_4 和$(Z_{12}^*,\cdot)$的意义：K_4 是 Klein 四元群(见主教材例 2.1.4)，$(Z_{12}^*,\cdot)$是整数模 12 的乘法群(例 2.1.6).

证 首先写出它们的元素：

$$K_4=\{e,a,b,c\},\quad Z_{12}^*=\{1,5,7,11\}.$$

作映射 $f:e\to1,a\to5,b\to7,c\to11$.

可以一一验证(略)满足

$$f(xy)=f(x)f(y).$$

所以 $K_4\cong(Z_{12}^*,\cdot)$.

点评 以上证明方法是完全按照同构的定义来证，我们也可以用生成群来证明此题. 由于 Klein 四元群就是 D_2，可定义为

$$K_4=\langle a,b\mid o(a)=o(b)=2,ba=ab\rangle,$$

而$(Z_{12}^*,\cdot)$可表示为

$$(Z_{12}^*,\cdot)=\langle 5,7\mid o(5)=o(7)=2,5\times7=7\times5\rangle\cong K_4.$$

作映射 $f:a\to5,b\to7$，则有 $f(e)=f(aa)=f(a)f(a)=1$，$f(c)=f(ab)=f(a)f(b)=35\bmod 12=11$. 这种方法可推广到其他的生成群.

2.3-4 $(\mathbb{Q}^+,\cdot)$和$(\mathbb{Q},+)$是否同构？

分析 先熟悉一下记号：$(\mathbb{Q}^+,\cdot)$是正有理数的乘法群，$(\mathbb{Q},+)$是有理数的加法群. 然后可先猜一下，结论是肯定还是否定. 感觉上似乎是否定，于是先按否定来证.

答 否！

证明如下：反证法.

假设有同构 $f:(\mathbb{Q},+)\to(\mathbb{Q}^+,\cdot)$.

设 $f(a)=2$，则 $f\left(\frac{a}{2}+\frac{a}{2}\right)=f\left(\frac{a}{2}\right)f\left(\frac{a}{2}\right)=2$，由此得

$$f\left(\frac{a}{2}\right)=\sqrt{2}\notin\mathbb{Q}^{+},\quad 矛盾.$$

所以不存在($\mathbb{Q}^{+}$,·)到($\mathbb{Q}$,+)的同构映射,因而($\mathbb{Q}^{+}$,·)和($\mathbb{Q}$,+)不同构.

点评 如果把$\mathbb{Q}$换成$\mathbb{R}$不难证明它们是同构的.请大家自己证明.

2.3-5 $G=\langle a\rangle$为无限循环群,$A=\langle a^s\rangle$,$B=\langle a^t\rangle$,证明:

(1) $A\cap B=\langle a^m\rangle$,$m=[s,t]$(最小公倍数);

(2) $\langle A,B\rangle=\langle a^d\rangle$,$d=(s,t)$(最大公因子).

分析 首先,s,t可理解为正整数,因为$A=\langle a^s\rangle$,则$(a^s)^{-1}=a^{-s}\in A$,s,$-s$中必有一个是正整数.

其次,记号$\langle A,B\rangle$表示由A与B中的元素生成的子群,与记号$\langle A\cup B\rangle$是相同的,即$\langle A,B\rangle=\langle A\cup B\rangle$.

再次,由于循环群有固定结构,我们可以把它转化为具体的群来分析.

另外,要证明两个集合相等,通常的方法是证明它们互相包含.

证 因为无限循环群都同构于($\mathbb{Z}$,+),故问题变为:$A=\langle s\rangle$,$B=\langle t\rangle$,证明:

(1) $A\cap B=\langle m\rangle$,$m=[s,t]$; (2) $\langle A,B\rangle=\langle d\rangle$,$d=(s,t)$.

用互相包含的方法证明此二等式.

(1) 任取$x\in A\cap B$,则$x=ps=qt$,x是s与t的公倍数,故$m\mid x$,因而$x\in\langle m\rangle$,所以$A\cap B\leqslant\langle m\rangle$.

反之,$\forall x\in\langle m\rangle$,可设$x=rm$.又因为$m\in A$和$m\in B$,得$m\in A\cap B$.故$x=rm\in A\cap B$.所以$\langle m\rangle\leqslant A\cap B$.

综上,得$A\cap B=\langle m\rangle$,表示成乘法循环群的形式就是$A\cap B=\langle a^m\rangle$,$m=[s,t]$(最小公倍数).

(2) 任取$x\in\langle A,B\rangle$,则x可表为$x=ps+qt$,因而$d\mid(ps+qt)\Rightarrow d\mid x$,得$x\in\langle d\rangle$,所以$\langle A,B\rangle\leqslant\langle d\rangle$.

反之,由最大公因子定理,存在$p,q\in\mathbb{Z}$使$d=ps+qt$,因而$d\in\langle A,B\rangle$,所以$\langle d\rangle\leqslant\langle A,B\rangle$.

综上,得$\langle A,B\rangle=\langle d\rangle$,表示成乘法循环群的形式就是$\langle A,B\rangle=\langle a^d\rangle$,$d=(s,t)$(最大公因子).

点评 用循环群的抽象表示法来证明此题,过程完全一样,只是书写麻烦一些,运算在指数上进行.读者不妨自己重证一遍.

我们还可把该题推广到有限循环群:设$G=\langle a\rangle$为n阶循环群,$s\mid n$,$t\mid n$,$A=\langle a^s\rangle$,$B=\langle a^t\rangle$(s,t理解为正整数),证明:

(1) $A\cap B=\langle a^m\rangle, m=[s,t]$(最小公倍数);

(2) $\langle A,B\rangle=\langle a^d\rangle, d=(s,t)$(最大公因子).

证明方法完全类似,首先把 n 阶循环群表示为:$G=(Z_n,+), s|n, t|n$,于是有 $A=\langle\bar{s}\rangle=\{\bar{0},\bar{s},\overline{2s},\cdots\}, B=\langle\bar{t}\rangle=\{\bar{0},\bar{t},\overline{2t},\cdots\}$,以下证明请读者自己完成.我们不妨举个例子来看一看:设 $G=(Z_{24},+)$,取 $s=4, t=6, A=\{\bar{0},\bar{4},\bar{8},\cdots,\overline{20}\}, B=\{\bar{0},\bar{6},\overline{12},\overline{18}\}$.则 $m=[4,6]=12, d=(4,6)=2$.所以 $A\cap B=\langle\overline{12}\rangle=\{\bar{0},\overline{12}\}, \langle A,B\rangle=\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4},\cdots,\overline{12}\}$.很容易验证,是对的.

学习近世代数的方法与学习初等代数有相同与不同的地方,不同的地方在于近世代数很抽象,要经常把抽象的理论与具体的例子结合起来,用具体的例子来想象抽象的规律.还有我们没有时间做很多类似的题,做完一个题,应联想到类似的问题如何做,是否还有其他的方法,需要更多的联想思考和更多的举一反三.

2.3-6　设 $G=\left\{\begin{bmatrix}1 & n\\ 0 & \pm 1\end{bmatrix} \middle| n\in\mathbb{Z}\right\}, A=\begin{bmatrix}1 & 1\\ 0 & -1\end{bmatrix}, B=\begin{bmatrix}1 & 2\\ 0 & -1\end{bmatrix}$,证明 $G=\langle A,B\rangle$.

分析　这是一个2次线性群的例子,而且其中的元素是二阶上三角矩阵,运算更加简单.证明方法主要是将 G 中任何元素用 A 和 B 来表示,从而证明两边互相包含.

证　方法类似于主教材例2.3.1.

首先,显然有 $\langle A,B\rangle\leqslant G$.

反之,任取 $X=\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}, Y=\begin{bmatrix}1 & n\\ 0 & -1\end{bmatrix}\in G$.令 $C=AB=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$,则有

$$X=\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}=C^n,\quad Y=\begin{bmatrix}1 & n\\ 0 & -1\end{bmatrix}=AC^{n-1},$$

因而 $X,Y\in\langle A,B\rangle$,所以 $G\subseteq\langle A,B\rangle$.

综上,得 $G=\langle A,B\rangle$.

点评　对矩阵的运算应该很熟练,特别是二阶矩阵,例如有一个求逆公式如下:

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}^{-1}=\frac{1}{ad-bc}\begin{bmatrix}d & -b\\ -c & a\end{bmatrix}.$$

2.3-7　非平凡子群 M 称为群 G 的极大子群,如果有子群 H 满足 $M<H\leqslant G$,则必有 $H=G$.确定无限循环群的全部极大子群.

分析　所谓"极大子群",是指包含关系的极大,具体定义为,若子群 M 满

足：(1)$M\neq G$；(2)若对任何 $H, M<H\leqslant G$ 都有 $H=G$. 则称 M 是 G 的一个极大子群.

由于无限循环群的全部子群我们都已知道了，原则上只要从中把那些极大子群挑出来就可以了.

解 首先把无限循环群写成：$G=(\mathbb{Z},+)$，而它的全部子群已知道，它的全部子群为

$$H_n=\langle n\rangle,\quad n=0,1,2,\cdots.$$

怎样从中找出极大子群呢？有若干种思路，下面介绍几种方法：

方法 1 要有一点直观的感觉和猜想. 整数 n 分合数与素数两类，因此我们分两种情形讨论. 通过简单的分析：当 n 是合数时，$\langle n\rangle$ 不是极大子群. 因而可猜想：当 n 是素数时，$\langle n\rangle$ 是极大子群. 证明如下：

设 p 为素数，若有子群 H 满足：$\langle p\rangle<H\leqslant G$，设 $H=\langle n\rangle$，则由 $p\nmid n$ 得 $(p,n)=1$，存在 r,s 使 $rp+sn=1$，因而得 $1\in H$，从而 $H=G$. 所以 $\langle p\rangle$ 是极大子群.

故 G 的全部极大子群为

$$\langle p\rangle,\quad p \text{ 为素数}.$$

方法 2 从极大子群的定义入手.

设 $M=\langle m\rangle, m\in\mathbb{Z}^+$ 是 G 的一个极大子群，则 $1<M<G$. 任取 $b\in G\backslash M$，令 $H=\langle M,b\rangle$. 显然 $M<H$，由极大子群的定义，得 $H=\langle M,b\rangle=G$，故存在 $u, v\in\mathbb{Z}$，使 $um+vb=1$，由此得 $(m,b)=1$. 由于 b 可取 $1,\cdots,m-1$ 中的任意数，即 m 与 $1,\cdots,m-1$ 都互素，因此 m 是素数.

所以 G 的全部极大子群为

$$\langle p\rangle,\quad p \text{ 为素数}.$$

点评 素数在近世代数中扮演很重要的角色，我们必须对第 1 章中有关内容非常熟悉.

如上一题的点评指出的那样，我们可以把本题推广到有限循环群，确定有限循环群的全部极大子群. 具体的结论与证明留给大家自己去完成，我们还是来看一个例子.

确定 $G=(Z_{24},+)$ 的全部极大子群. 不难看出它的全部极大子群为：$\langle\overline{2}\rangle,\langle\overline{3}\rangle$.

2.3-8 设 p 为素数，$G=\{x\in\mathbb{C}\mid x^{p^n}=1, n=1,2,\cdots\}$ 是对复数乘法的群，证明 G 的任何真子群是有限循环群.

分析 先把这个群的元素搞清楚，G 的每一个元素是 p^n 次单位复数根，且 n 可为任意正整数. 我们先看看封闭性，设 α 是 p^s 次单位复数根，β 是 p^t 次

单位复数根，如果 $s\geqslant t$，则 $(\alpha\beta)^{p^s}=1$，所以 $\alpha\beta\in G$. 但是 G 不是循环群，要证它的任何真子群是有限循环群. 关键是从真子群入手.

证　虽然 G 不是循环群，但对于固定的 n 由所有 p^n 次单位复数根形成的群是有限循环群，因而只要证明任何一个真子群必是某个 n 的所有 p^n 次单位根形成的群就可以了. 这里的真子群的概念指的是真包含的意思.

由于 p^n 次单位复数根可表示出来，所以 G 可表示为

$$G=\{e^{i\frac{2k\pi}{p^n}}\mid 0\leqslant k<p^n,n\in\mathbb{Z}^+\}.$$

设 H 是 G 的任一真子群，由于 H 是真子群，必有一元素 $e^{i\frac{2q\pi}{p^m}}$ 且 $(q,p)=1$ 不属于 H，由此可得所有的元素 $e^{i\frac{2k\pi}{p^n}}$，$(k,p)=1$，$n\geqslant m$，都不属于 H（为什么?）. 令

$$S=\{e^{i\frac{2k\pi}{p^n}}\mid (k,p)=1,n\geqslant m\},$$

则 $H\subseteq G\backslash S$，而 $G\backslash S$ 可表为

$$G\backslash S=\left\{e^{i\frac{2k\pi}{p^n}}\,\middle|\,0\leqslant k<p^n,n<m\right\}\subset\left\{e^{i\frac{2k\pi}{p^m}}\,\middle|\,0\leqslant k<p^m\right\}$$

$$=\langle e^{i\frac{2\pi}{p^m}}\rangle=K,$$

K 是 p^m 阶循环群，而 $H<K$，由于循环群的子群仍是循环群，所以 H 是有限循环群.

点评　此题涉及单位复数根的问题，读者应对单位复数根和单位复数原根有所了解.

***2.3-9**　$G=\langle A,B\rangle$，$A=\begin{bmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\ddots&\ddots&\vdots\\0&0&\cdots&0&1\\1&0&0&\cdots&0\end{bmatrix}$，　$B=\begin{bmatrix}1&0&0&\cdots&0\\0&\omega&0&\cdots&0\\0&\ddots&\omega^2&\ddots&\vdots\\\vdots&\vdots&\ddots&\ddots&\vdots\\0&0&\cdots&0&\omega^{n-1}\end{bmatrix}$，其中 ω 为 n 次单位原根. 证明 $|G|=n^3$.

分析　这是由两个元素生成的群，类似于本节第1题，如果能通过交换生成元写出群元素的一般形式，则问题就能解决.

解　为了写出群元素的一般形式，通过计算 A 与 B 的乘积来分析，由于 B 是一个对角矩阵，用它做乘法很简单，A 与 B 的阶数都是 n，可以得到

$$BA=\omega^{-1}AB,$$

因而 G 可表示为

$$G=\{\omega^i A^j B^k \mid i,j,k=0,1,\cdots,n-1\},$$

所以 $|G|=n^3$.

点评 对于由两个元素生成的群,通常用这种方法来写出它的全部元素. 在证明过程中有一点还不太严格,就是需要证明:

$$\omega^i A^j B^k=\omega^r A^s B^t \Leftrightarrow (i,j,k)=(r,s,t).$$

$$\omega^i A^j B^k=\omega^r A^s B^t \Leftrightarrow \omega^{i-r}A^{j-s}B^{k-t}=e\Leftrightarrow$$

由两边求行列式,得 $\omega^{i-r}=1$,所以 $i=r$,$A^jB^k=A^sB^t \Leftrightarrow A^{j-s}B^{k-t}=I$

$\Leftrightarrow k-t\equiv 0 \pmod n$,$j-s\equiv 0\pmod n$,考虑到取值范围,得 $k=t$,$j=s$.

2.4 变换群和置换群,Caylay 定理

一、内容提要

变换群和置换群是第三大类群(第一类是数群和整数同余类群,第二类是线性群),它实质上类似于微积分中的函数. 不过,微积分重点研究的是实连续函数,即$\mathbb{R}$ 到$\mathbb{R}$ 的变换. 而群论的研究对象本质上是有限集或无限集上的变换,且重点研究的是有限集上的变换. 置换就是有限集上的可逆变换,设 $B=\{1,2,\cdots,n\}$,则 B 上的一个双射称为一个 n 次置换,B 称为目标集. 又由 Cayley 定理可知,任何群都同构于变换群或置换群,所以,置换群代表了所有的有限群,是群论的重要研究对象.

1. 置换的表示方法和分类

(1) 任一 n 次置换可表示为不相交的轮换之积

$\sigma=(i_1,\cdots,i_{l_1})(j_1,\cdots,j_{l_2})\cdots(t_1,\cdots,t_{l_s})$(长度为 1 的轮换,称为 σ 的不动点,可以略去). 每个轮换 $(i_1,\cdots,i_l)$ 的表示方法不惟一:

$$(i_1,i_2\cdots,i_l)=(i_2,\cdots,i_l,i_1)=\cdots=(i_l,i_1\cdots,i_{l-1}),$$

只要保持循环次序不变,轮换可从任一元素开始.

一个置换的轮换表示在不计轮换的次序和不计轮换内谁打头的条件下是惟一的.

- 置换的类型:如果置换 σ 的轮换分解式中有 λ_k 个长度为 k 的轮换,$k=1,2,\cdots,n$.(满足:$1\cdot\lambda_1+2\cdot\lambda_2+\cdots+n\cdot\lambda_n=n$). 则称 σ 是一个 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$-型置换. $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$-型置换的个数为

$$\frac{n!}{1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\lambda_1!\lambda_2!\cdots\lambda_n!}.$$

- σ 的阶数：单个轮换的阶数等于其长度. $o(\sigma)=[l_1,l_2,\cdots,l_s]$(最小公倍数.)

(2) **任一 n 次置换可表示为对换之积**

$$\sigma=(i_1,j_1)(i_2,j_2)\cdots(i_s,j_s),$$

其中的对换可以相交,表示方法不惟一,但所含对换个数 s 的奇偶性是惟一确定的.

- σ 的奇偶性 $=\sum_{k=1}^{s}(l_k-1)$ 的奇偶性 $=s$ 的奇偶性(即对换个数的奇偶性). 用式子表达就是

$$\sum_{k=1}^{s}(l_k-1)\equiv s(\text{mod }2).$$

单位置换记作 $e=(1)$,阶数为 1,是偶置换.

提醒：单个轮换 $\sigma=(i_1,\cdots,i_l)$的奇偶性与其长度的奇偶性相反.

- 一个二阶置换必可表为不相交的对换之积.

2. 置换的运算

置换的乘法及乘积的奇偶性规则必须熟练掌握！本书规定置换的乘法由右向左进行.

3. 置换群

- n 次对称群 S_n=全体 n 次置换,n 次交错群 A_n=全体 n 次偶置换. S_n 的任何子群称为置换群.
- 任何一个置换群或由偶置换组成,或奇、偶置换各半.
- 某些置换群的几何意义：正多边形的旋转群 D_n,正多面体的旋转群.
- 置换群的生成元的一个重要公式：

$$S_n=\langle(12),(13),\cdots,(1n)\rangle.$$

注意此公式的证明方法主要有两点：一是把任何一个置换表示为对换之积,二是把每一个对换表示为生成元的乘积. 这两个方法可推广用于证明其他公式(见习题 2.4.4 和习题 2.4.5).

4. Cayley 定理

任何一个群(有限群)G 同构于一个变换(置换)群.

在证明过程中我们用了一个 G 上的变换：$f_a:x\mapsto ax\,(G\to G)$,从而证明

$$G\cong\{f_a\mid f_a(x)=ax\,(G\to G),a\in G\}.$$

变换 $f_a: x \mapsto ax(G \to G)$ 称为 G 上的左平移变换（f_a 在 G 上没有不动点）. 类似地，也可以用 G 上的右平移变换 $g_a: x \mapsto xa^{-1}(G \to G)$ 来证明定理（是否可用变换 $x \mapsto xa$?）. 但不可以用共轭变换来证明此定理（为什么?）. 定理的证明过程提供了一个把任意一个群转换为一个变换群或置换群的方法.

二、习题 2.4 详细解答

2.4-1 设 $\sigma = (i_1, i_2, \cdots, i_k)$，$\tau \in S_n$，证明

$$\tau\sigma\tau^{-1} = (\tau(i_1), \tau(i_2), \cdots, \tau(i_k)).$$

分析 该题主要练习置换与轮换的记号与运算. 首先要把题目看懂，搞清要证明什么? 要证两点：

(1) 对于任何 $j \in \{\tau(i_1), \tau(i_2), \cdots, \tau(i_k)\}$（注意花括号与圆括号的区别）有

$$\tau\sigma\tau^{-1}(\tau(i_m)) = \tau(i_{m+1}), \quad m = 1, 2, \cdots, k-1; \quad \tau\sigma\tau^{-1}(\tau(i_k)) = \tau(i_1).$$

(2) 对于任何 $j \notin \{\tau(i_1), \tau(i_2), \cdots, \tau(i_k)\}$ 有

$$\tau\sigma\tau^{-1}(j) = j, \quad \text{即 } j \text{ 是 } \tau\sigma\tau^{-1} \text{ 的不动点}.$$

（为什么还要证明(2)?）

证 具体证明如下：

(1) 对于任何 $j \in \{\tau(i_1), \tau(i_2), \cdots, \tau(i_k)\}$，利用置换的结合律，有

$$\tau\sigma\tau^{-1}(\tau(i_m)) = \tau\sigma(i_m) = \tau(i_{m+1}), \quad m = 1, 2, \cdots, k-1.$$

$$\tau\sigma\tau^{-1}(\tau(i_k)) = \tau\sigma(i_k) = \tau(i_1).$$

(2) 对于任何 $j \notin \{\tau(i_1), \tau(i_2), \cdots, \tau(i_k)\}$，设 $j = \tau(i)$，则 $i \notin \{i_1, i_2, \cdots, i_k\}$，$\sigma(i) = i$，因而

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau\sigma(i) = \tau(i), \quad \text{即} \quad \tau\sigma\tau^{-1}(j) = j.$$

综上得证.

另一证法：上面的证法中利用置换的轮换形式，由于对某一置换的不动点不出现在轮换中，因而需分两种情况. 如果采用置换的双行形式，则证明反而可简单一些.

σ 可表为

$$\sigma = \begin{pmatrix} i_1 \cdots i_2 \cdots i_k \cdots \\ i_2 \cdots i_3 \cdots i_1 \cdots \end{pmatrix},$$

设 $\tau(i_m) = j_m$，$m = 1, 2, \cdots, k$，则 τ 可表为

$$\tau = \begin{pmatrix} i_1 \cdots i_2 \cdots i_k \cdots \\ j_1 \cdots j_2 \cdots j_k \cdots \end{pmatrix},$$

作运算

$$\tau\sigma\tau^{-1} = \begin{pmatrix} i_1 \cdots i_2 \cdots i_k \cdots \\ j_1 \cdots j_2 \cdots j_k \cdots \end{pmatrix} \begin{pmatrix} i_1 \cdots i_2 \cdots i_k \cdots \\ i_2 \cdots i_3 \cdots i_1 \cdots \end{pmatrix} \begin{pmatrix} j_1 \cdots j_2 \cdots j_k \cdots \\ i_1 \cdots i_2 \cdots i_k \cdots \end{pmatrix}$$

$$= \begin{pmatrix} j_1 \cdots j_2 \cdots j_k \cdots \\ j_2 \cdots j_3 \cdots j_1 \cdots \end{pmatrix} = (j_1, j_2, \cdots, j_k) = (\tau(i_1), \tau(i_2), \cdots, \tau(i_k)).$$

点评 通过这个题,我们对置换的两种表示方法应搞清楚,对它们的运算方法应掌握.我们规定乘积是从右向左进行,但有的书规定是从左向右进行的.我们看参考书时应多加注意.

该题还给出置换运算的一个重要规律.我们把 $\tau\sigma\tau^{-1}$ 称为用 τ 对 σ 作**共轭运算**,设 $\tau\sigma\tau^{-1}=\sigma_1$,则称 σ 与 σ_1 共轭.因此本题给出的公式:$\sigma=(i_1, i_2, \cdots, i_k)$,$\tau \in S_n$,则

$$\tau\sigma\tau^{-1} = \tau(i_1, i_2, \cdots, i_k)\tau^{-1} = (\tau(i_1), \tau(i_2), \cdots, \tau(i_k)).$$

我们称此公式为**置换的共轭变换公式**.它非常重要,一定要记住!(虽然大家已是学海老手,不该像小学生那样经常要求死背一些东西,但学任何一门课,如果不记住一些最基本的东西,可能很难进行下去.)

共轭的概念可推广到任何群中,在线性群中共轭就是大家熟悉的相似运算.那么本题的结果,就是对轮换作共轭运算后仍是一个轮换,且长度不变.并由此可得,对任何置换作共轭运算,将保持类型不变:设 $\sigma=(i_1, \cdots, i_{l_1})(j_1, \cdots, j_{l_2})\cdots(t_1, \cdots, t_{l_s})$,则由本题的结果,对任意置换 τ 有

$$\begin{aligned}\tau\sigma\tau^{-1} &= \tau(i_1, \cdots, i_{l_1})\tau^{-1}\tau(j_1, \cdots, j_{l_2})\tau^{-1}\cdots\tau(t_1, \cdots, t_{l_s})\tau^{-1} \\ &= (\tau(i_1), \cdots, \tau(i_{l_1}))(\tau(j_1), \cdots, \tau(j_{l_2}))\cdots(\tau(t_1), \cdots, \tau(t_{l_s})).\end{aligned}$$

因而类型不变.

共轭运算与元素的可交换性有密切的关系,以下两点在分析群的结构时有用:

(1) $bab^{-1}=a \Leftrightarrow ba=ab$;

(2) $bab^{-1}=a^s \Leftrightarrow ba=a^s b$.(可称为准交换性)

利用此性质可将由两个元素生成的群简化,这在二面体群中已经用到过.

2.4-2 证明 $|A_n|=\dfrac{n!}{2}$.

分析 此题实际上要证 A_n 的元素个数是 S_n 的元素个数的一半,或 S_n 中奇置换的个数与偶置换的个数相等.为此我们来找偶置换的集合与奇置换的集合之间的关系.

证 设 B 为 S_n 中全体奇置换的集合,任取奇置换 $\sigma \in B$,记

$$\sigma B = \{\sigma\tau \mid \tau \in B\},$$

(见主教材 2.2 节子集运算的意义,即式(2.2.1) ~ (2.2.3))

则由于两个奇置换的乘积是偶置换，得 $\sigma B\subseteq A_n$，因而

$$|\sigma B|=|B|\leqslant|A_n|. \quad (\text{为什么 } |\sigma B|=|B|?)$$

反之，由于奇置换与偶置换的乘积是奇置换，得 $\sigma A_n\subseteq B$，因而

$$|\sigma A_n|=|A_n|\leqslant|B|.$$

综上，得

$$|A_n|=|B|=\frac{n!}{2}.$$

即 S_n 中奇、偶置换各半.

点评 通过此题进一步了解对称群的结构，奇、偶置换运算的规则，熟悉元素与子群乘积的记号. 此题的结论可推广到一般的置换群，见下一题.

2.4-3 证明任何一个置换群的元素或全部元素均为偶置换，或奇、偶置换各半.

分析 方法与上题类似.

证 只需证明当置换群中含有奇置换时，必为奇、偶置换各半.

设群 G 含有奇置换，令

A 为 G 中全体偶置换的集合，B 为 G 中全体奇置换的集合.

它们均为非空. 任取 $\sigma\in B$，则 $\sigma A\subseteq B$，因而 $|\sigma A|=|A|\leqslant|B|$；类似地，由于 $\sigma B\subseteq A$，得 $|\sigma B|=|B|\leqslant|A|$. 所以

$$|A|=|B|=\frac{|G|}{2}.$$

点评 此题比上题更为简单，只是为了对置换群的结构加深印象.

2.4-4 证明 $S_n=\langle(12),(123\cdots n)\rangle$.

分析 这也是一个经典的公式，参看本节例 2.4.4. 注意熟悉生成群和生成元的意义、置换的乘法运算. 并可利用本节习题第 1 题的共轭运算公式.

证 我们可以利用本节例 2.4.4 的结果：

$$S_n=\langle(12),(13),\cdots,(1n)\rangle.$$

只要证明 $(1i)$ 可由 (12)，$(123\cdots n)$ 生成.

利用共轭运算公式，令

$$\sigma=(12), \quad \tau=(123\cdots n).$$

则由共轭运算公式得

$$\tau\sigma\tau^{-1}=(\tau(1),\tau(2))=(23), \quad \sigma(23)\sigma^{-1}=(\sigma(2),\sigma(3))=(13),$$

类似方法可得到其他的 $(1i)$. 所以

$$\langle\sigma,\tau\rangle=\langle(12),(13),\cdots,(1n)\rangle=S_n.$$

点评 有了共轭运算公式使我们多了一种运算工具，比盲目用凑和试的方法更先进一些.

2.4-5 证明 $A_n=\langle(123),(124),\cdots,(12n)\rangle$.

分析 这也是一个经典的公式. 可用刚刚掌握的共轭运算公式来做.

证 方法类似于上题. 但要利用偶置换的性质.

显然，$\langle(123),(124),\cdots,(12n)\rangle\leqslant A_n$，因此只要证明对任何 $\sigma\in A_n$ 有 $\sigma\in\langle(123),(124),\cdots,(12n)\rangle$.

任取 $\sigma\in A_n$，σ 可表示为偶数个对换之积：

$$\sigma=(1i_1)(1j_1)(1i_2)(1j_2)\cdots(1i_m)(1j_m).$$

我们来分析每一对对换 $(1i),(1j)$，如何用 $(12i)$ 和 $(12j)$ 来生成，取 $\sigma=(12j)$，$\tau=(12i)^{-1}=(1i2)$，则

$$\tau\sigma\tau^{-1}=(1i2)(12j)(12i)=(1ji)=(1i)(1j),$$

因此每一对对换 $(1i),(1j)$ 都可用 $(12i)$ 和 $(12j)$ 来表示，所以

$$\sigma\in\langle(123),(124),\cdots,(12n)\rangle.$$

这样就证明了

$$A_n=\langle(123),(124),\cdots,(12n)\rangle.$$

点评 仔细体会所用的方法，方法不是惟一的，需要一定的试验. 这种方法在以后的内容里要反复用到.

2.4-6 求出正四面体的旋转群.

分析 方法类似本节例 2.4.2.

解 可先作一个正四面体的图，顶点为 1，2，3，4. 每一个绕对称轴旋转且保持空间位置不变的变换，对应一个四元置换. 所有这样的置换构成正四面体的旋转群.

它的对称轴可分两类：

第一类为过一顶点和底面中心的轴分别旋转 120°和 240°，这样的旋转有

$$(1),(234),(243),(134),(143),(124),(142),(123),(132).$$

第二类为过两条对边的中点的轴，旋转 180°，这样的旋转有

$$(12)(34),(13)(24),(14)(23).$$

所以正四面体的旋转群为

$$G=\{(1),(234),(243),(134),(143),(124),(142),(123),(132),\\(12)(34),(13)(24),(14)(23)\}=A_4.$$

点评 很容易丢了第二类旋转. 为了避免丢失，我们可以先计算旋转群应有的元素个数，一直找到所有的元素为止. 计算旋转群应有的元素个数的方法将在以后介绍.

2.4-7 证明正立方体的旋转群同构于 S_4.

分析 先把正立方体的旋转群的所有元素写出来,然后找出它们与 S_4 的元素的对应关系.但这种方法比较乱,不容易找出对应关系.我们可从几何意义出发,看能否把 8 个顶点的置换变成某 4 个元素的置换.

证 正立方体的旋转群在本节中已求出,共有 24 个元素,与 S_4 的元素个数相同.但如何找到它们的元素之间的对应关系呢?主要的问题在于,正立方体的旋转群的基集有 8 个元素,而 S_4 的基集有 4 个元素.为此,我们可把正立方体的 8 个顶点按对顶点两两一组分为 4 组,分组的原则是在旋转过程中始终在一起,在几何上意味着每一组代表一根轴(见主教材图 2.2),于是 8 个顶点的一个置换就变成四根轴的一个置换.例如可取以下分组方法:

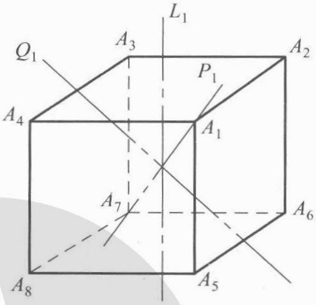


图 2.3

令 $a=\{1,7\}$, $b=\{2,8\}$, $c=\{3,5\}$, $d=\{4,6\}$,在几何上它们对应过对顶点的四根轴,则可把正立方体的旋转群的每一个元素变为集合$\{a,b,c,d\}$上的一个置换,例如,

$$(1234)(5678)\to(abcd),$$
$$(13)(24)(57)(68)\to(ac)(bd),$$
$$(245)(386)\to(bdc),$$
$$(12)(78)(35)(46)\to(ab),\text{等等}.$$

由于从几何意义上看,是同一个群,所以它们同构.

点评 如果按同构的定义来证明,是一件非常复杂的事情,因为要证明保持运算需要验证$\binom{n}{2}$个式子,所以通常通过分析群的结构来证明两个群是否同构.

2.4-8 确定 S_n 中长度为 n 的轮换个数.

分析 可以直接求,注意到一个轮换与哪一个元素打头无关,因此可把某个元素固定在第一个.也可以套公式.

解 **方法 1** 直接求. S_n 中长度为 n 的轮换可表示为

$$(1,i_2,i_3,\cdots,i_n).$$

由于 $i_2,i_3,\cdots,i_n$ 为 $2,3,\cdots,n$ 的任一排列,所以 S_n 中长度为 n 的轮换的个数等于 $n-1$ 阶全排列数:$(n-1)!$.

方法 2 代公式. S_n 中长度为 n 的轮换是 n^1-型置换,由本节公式得个

数为

$$\frac{n!}{n}=(n-1)!.$$

点评 对于类型复杂的置换,还是用公式好.因为直接求就是推导公式.例如,设 $d|n$,求 $d^{\frac{n}{d}}$-型置换的个数.由公式得其个数为

$$\frac{n!}{d^{\frac{n}{d}}\left(\frac{n}{d}\right)!},$$

设 $n=dk$,则 $d^{\frac{n}{d}}$-型置换的个数为

$$\frac{n!}{d^k k!}=\frac{n(n-1)\cdots(n-k+1)}{d^k}.$$

不妨用具体数来验证一下.

问题:试求不含不动点的置换个数.(首先,把这个问题理解清楚,不妨用具体的 n 看一下.详细答案参考[4](3.8)式,或见本章补充题.)

2.5 子群的陪集和 Lagrange 定理

一、内容提要

1. 子群的陪集及其性质

- **陪集的定义**:$H\leqslant G, a\in G$, H 的左陪集:aH. H 的右陪集:Ha.
- **陪集相等的条件**:

左陪集:$aH=bH\Leftrightarrow a^{-1}b\in H\Leftrightarrow b\in aH\Leftrightarrow aH\cap bH\neq\varnothing$.

右陪集:$Ha=Hb\Leftrightarrow ab^{-1}\in H\Leftrightarrow b\in Ha\Leftrightarrow Ha\cap Hb\neq\varnothing$.

对加群$(G,+)$,左陪集和右陪集相等,并记作 $a+H$.

- **由陪集所决定的等价关系**:

$$a\sim_L b\Leftrightarrow aH=bH\Leftrightarrow\cdots,$$
$$a\sim_R b\Leftrightarrow Ha=Hb\Leftrightarrow\cdots.$$

- **商集**:子群的陪集集合

$$\{aH\mid a\in G\}=G/\sim_L=(G/H)_L,\quad \{Ha\mid a\in G\}=G/\sim_R=(G/H)_R.$$

- **左、右陪集之间的关系**:左、右陪集之间存在双射 $f:aH\mapsto Ha^{-1}$.

2. 子群的指数与 Lagrange 定理

(1) **子群的指数**:就是子群的陪集的个数:$H\leqslant G$, $[G:H]=|\{aH|a\in G\}|$.指数有无限和有限两种情况.对有限群,指数也是有限的.

(2) **Lagrange 定理**：当 $|G|<\infty$，$H\leqslant G$ 时，$|G|=|H|[G:H]$.

(3) **子群的指数性质与应用**：

① 当 $|G|<\infty$ 时，$|H|\,\big|\,|G|$ 和 $\forall a\in G$ 有 $o(a)\,\big|\,|G|$.

② **望远镜公式**：$K\leqslant H\leqslant G$，则 $[G:K]=[G:H][H:K]$.（后面的习题）

3. 若干结果

- 素数阶群必为循环群.
- **Euler(欧拉)定理**：$a\in\mathbb{Z}^*$，$n>1$ 的整数，且 $(a,n)=1$，则 $a^{\varphi(n)}\equiv 1(\mathrm{mod}\ n)$.
- **Welson 定理**：p 为素数，则 $(p-1)!\equiv -1(\mathrm{mod}\ p)$.
- **有限子群乘积的基数**：$A,B\leqslant G$ 且 $|A|,|B|<\infty$，则 $|AB|=\dfrac{|A||B|}{|A\cap B|}$.
- **四阶群只有两种情况**：四阶循环群和 Klein 四元群. 它们都是可换群.

二、习题 2.5 详细解答

2.5-1 设 $H\leqslant G$，$a,b\in G$，证明以下命题等价：

(1) $a^{-1}b\in H$，(2) $b\in aH$，(3) $aH=bH$，(4) $aH\cap bH\neq\varnothing$.

分析 一般证明多个等价的命题采用循环证法.

证 本题主要熟悉陪集性质. 用循环证法.

(1) =>(2)：$a^{-1}b\in H\Rightarrow a^{-1}b=h\Rightarrow b=ah\Rightarrow b\in aH$.

(2) =>(3)：$b\in aH\Rightarrow bh\in aH\Rightarrow bH\subseteq aH$.

另一方面，$b\in aH\Rightarrow b=ah_1\Rightarrow a=bh_1^{-1}\in bH\Rightarrow aH\subseteq bH$.

综上得 $aH=bH$.

(3) =>(4)：$aH=bH$ 显然有 $aH\cap bH\neq\varnothing$.

(4) =>(1)：$aH\cap bH\neq\varnothing$ => 存在 $h_1,h_2\in H$ 使 $ah_1=bh_2$，所以 $a^{-1}b=h_1h_2^{-1}\in H$.

证毕.

点评 陪集的性质非常重要，该题可以改为对右陪集的类似命题，但条件 $a^{-1}b\in H$ 要改为 $ab^{-1}\in H$，所以条件 $a^{-1}b\in H$ 中 -1 的位置不可随意改变. 这与共轭条件不同，两元素共轭条件既可写为 $gag^{-1}=b$，也可写为 $g^{-1}ag=b$.

2.5-2 $G=\{a_1a_2a_3a_4a_5\mid a_i=0$ 或 $1\}$，G 的加法运算+定义为二进制按位加法(不进位). $H=\{00000,10101,01011,11110\}$，写出 H 在 G 中的所有陪集.

分析 本题目的是熟悉陪集的计算.

解 不难检验 H 确为子群. 作陪集时,尽量先选简单的元素作为代表元,这样计算较为简单. 本题可选含1的个数较少的元素作代表元. 由此得 H 在 G 中的陪集为

$$00000+H=H,$$
$$00001+H=\{00001,10100,01010,11111\},$$
$$00010+H=\{00010,10111,01001,11100\},$$
$$00100+H=\{00100,10001,01111,11010\},$$
$$01000+H=\{01000,11101,00011,10110\},$$
$$10000+H=\{10000,00101,11011,01110\},$$
$$10010+H=\{10010,00111,11001,01100\},$$
$$11000+H=\{11000,01101,10011,00110\}.$$

应检验一下是否不重不漏.

2.5-3 确定 A_4 的全部子群.

分析 确定一个群的子群问题的方法主要是利用 Lagrange 定理,从子群的阶入手.

解 对有限群,子群的阶是群的阶的因子. 因此我们可以按子群的阶来找所有的子群. 由于 $|A_4|=12$,子群的阶只能是1,2,3,4,6,12. 对每一个子群,再利用元素的阶是群的阶的因子,用生成元表示.

一阶子群:$\{(1)\}$.

二阶子群:$\langle(12)(34)\rangle,\langle(13)(24)\rangle,\langle(14)(23)\rangle$.

三阶子群:$\langle(123)\rangle,\langle(124)\rangle,\langle(134)\rangle,\langle(234)\rangle$.

四阶子群:$\{(1),(12)(34),(13)(24),(14)(23)\}$.

六阶子群:由于 A_4 中无六阶元,故 A_4 中无六阶循环子群. A_4 中的六阶子群只能由一个二阶元和一个三阶元生成,可任取一个二阶元和任取一个三阶元,例如(12)(34)和(123),易证 $\langle(12)(34),(123)\rangle=A_4$. 所以 A_4 中无六阶子群.

十二阶子群:A_4.

点评 请读者用这种方法确定 S_4 的所有子群. 有一个问题不知是否已经解决,就是 S_4 和 A_4 中的子群的个数是多少?

2.5-4 $A,B\leqslant G$, $|A|<\infty$, $|B|<\infty$, $(|A|,|B|)=1$,证明 $|AB|=|A||B|$.

分析 显然,应想到利用有限子群乘积的基数公式(见主教材定理2.5.3):

$$|AB|=\frac{|A||B|}{|A\cap B|},$$

只需证明$|A\cap B|=1$.

证 由于$A\cap B\leqslant A$ 和$A\cap B\leqslant B$,故由 Lagrange 定理得,$|A\cap B|$能同时整除$|A|$和 $|B|$. 又由于$(|A|,|B|)=1$,所以$|A\cap B|=1$.

因此由有限子群乘积的基数公式得

$$|AB|=\frac{|A||B|}{|A\cap B|}=|A||B|.$$

点评 能否用映射的方法来证明此题: $f:ab\mapsto(a,b)(AB\to A\times B)$?

2.5-5 $A,B\leqslant G,C=\langle A\cup B\rangle$是由 $A\cup B$ 生成的子群,证明$[C:A]\geqslant[B:A\cap B]$.

分析 首先要看懂题意. C 是由 A 和 B 生成的子群: $C=\langle A\cup B\rangle=\langle A,B\rangle$. 子群指数$[C:A]$和$[B:A\cap B]$都是有限的,但群 G 与子群 A 和 B 不一定是有限的,所以不能直接利用主教材定理 2.5.3,但可利用它的证明方法(请查阅). 由于子群的指数等于子群的陪集的个数,可用两个子群的陪集集合之间的映射来揭示它们的数目之间的关系. 直观上可画一个图来看一下.

证 **方法 1** 令 $D=A\cap B,S=\{bD\mid b\in B\},T=\{cA\mid c\in C\}$,则$[B:A\cap B]=|S|,[C:A]=|T|$. 只需证明$|S|\leqslant|T|$,可用映射的方法来证明它.

作对应关系 f: $bD\mapsto bA(S\to T)$,

首先我们来证明 f 是映射: $b_1D=b_2D\Rightarrow b_1^{-1}b_2\in D\Rightarrow b_1^{-1}b_2\in A\Rightarrow b_1A=b_2A$. 并且上面的每一步均可倒推回去,所以 f 是单射. 因此$|S|\leqslant|T|$,即

$$[C:A]\geqslant[B:A\cap B].$$

方法 2 用 BA 作为中间集合.

首先,$BA\subseteq C$,令 $K=\{bA\mid b\in B\}$,则$|K|\leqslant[C:A]$. 令 $D=A\cap B,S=\{bD\mid b\in B\}$,则$[B:A\cap B]=|S|$.

作对应关系 $f:bD\mapsto bA(S\to K)$,

首先我们来证明 f 是映射: $b_1D=b_2D\Leftrightarrow b_1^{-1}b_2\in D\Leftrightarrow b_1^{-1}b_2\in A\Leftrightarrow b_1A=b_2A$. 所以 f 是映射且是单射. 显然是满射. 故有$|K|=|S|=[B:A\cap B]$. 所以

$$[C:A]\geqslant|K|=[B:A\cap B].$$

点评 注意定义对应关系 f 后,为什么还要证明它是映射?

这是因为二元关系不一定是映射. 由于陪集的表示方法不惟一,可能会产生一对多的问题. 凡是自变量表示方法不惟一时,当定义一个对应关系后,必

须证明它是否是映射.

另外,子群乘积可作陪集分解：$A,B\leqslant G, BA=\bigcup_{b\in B} bA$.

2.5-6　设 $A\leqslant G, B\leqslant G$,若有 $g,h\in G$ 使 $Ag=Bh$,则 $A=B$.

分析　采用互相包含的方法来证明集合相等.

证　为此先将 g 和 h 表达出来.

由 $Ag=Bh$ 可得,存在 $a\in A, b\in B$ 使 $g=bh, ag=h$,因而

$\forall x\in A$ 有 $y\in B$ 使 $xg=yh$,得 $x=yhg^{-1}=yhh^{-1}b^{-1}=yb^{-1}\in B$,所以 $A\subseteq B$.

反之,$\forall y\in B$ 有 $x\in A$ 使 $xg=yh$,得 $y=xgh^{-1}=xa^{-1}hh^{-1}=xa^{-1}\in A$,所以 $B\subseteq A$.

综上,得 $A=B$.

点评　此题主要用到群中元素的运算,是很基本的.

2.5-7　$A\leqslant B\leqslant G\Rightarrow[G:A]=[G:B][B:A]$.

分析　按题意,子群 A,B 的指数是有限的,但子群本身并不一定有限,所以不能套用 Lagrange 公式. 可以用证明 Lagrange 公式时所用的陪集分解来证明.

证　设$[G:B]=m,[B:A]=n$,则 G,B 可表示为

$$G=\bigcup_{i=1}^{m} g_iB,\quad B=\bigcup_{j=1}^{n} b_jA,$$

因而得

$$G=\bigcup_{i=1}^{m}\bigcup_{j=1}^{n} g_ib_jA.$$

下面证式中 mn 个陪集互不相交：由于

$$\begin{aligned} g_ib_jA &= g_kb_lA\Rightarrow b_j^{-1}g_i^{-1}g_kb_l \in A\Rightarrow g_i^{-1}g_k \in b_jAb_l^{-1}\\ &\Rightarrow g_i^{-1}g_k \in B\Rightarrow g_i = g_k\Rightarrow i = k\\ &\Rightarrow b_jA = b_lA\Rightarrow b_j = b_l\Rightarrow j = l. \end{aligned}$$

即$(i,j)\neq(k,l)\Leftrightarrow g_ib_jA\neq g_kb_lA\Leftrightarrow g_ib_jA\cap g_kb_lA=\varnothing$. 所以

$$[G:A] = mn = [G:B][B:A].$$

点评　该题最容易犯的错误是把 G 看作有限群,用 Lagrange 定理来证明. 此公式称为子群指数的**望远镜公式**,古代用的双节望远镜的放大倍数是两节放大倍数的乘积.

2.6　正规子群和商群

一、内容提要

正规子群的概念十分重要，是群论的核心内容之一. 通过正规子群可得到一个新的群.

1. 正规子群

正规子群就是左、右陪集相等的子群，并记作 $H \trianglelefteq G$. 有以下互相等价的条件. 设 $H \leqslant G$，则以下的条件互相等价：

(1) $\forall g \in G$ 有 $gH = Hg$.（左、右陪集相等——正规子群的定义）

(2) $\forall g \in G$ 和 $\forall h \in H$ 有 $ghg^{-1} \in H$.（H 的元素的所有共轭元仍在H 中）

(3) $\forall g \in G$ 有 $gHg^{-1} = H$.（所以正规子群又称自共轭子群，或不变子群）

(4) $\forall g \in G$ 有 $gHg^{-1} \subseteq H$.

要检验一个子群是否是正规子群，可用上面 4 个条件的任何一个. 但最常用的是条件(2).

正规子群的记号为 $H \trianglelefteq G$，当 $H \neq G$ 时（即真包含），记作 $H \triangleleft G$. 但有时在并不强调是否是真包含时，为了简单起见，都记作 $H \triangleleft G$.

当然，可交换群的任何子群都是正规子群.

2. 共轭元与共轭子群

元素的共轭运算与子群的共轭运算在群中有很重要的作用.

- 共轭元：a 与 b 共轭$\Leftrightarrow \exists\, g \in G$ 使 $gag^{-1} = b$（或 $g^{-1}ag = b$）.
- 元素的共轭关系是等价关系：a 与 b 共轭$\Leftrightarrow a \sim_c b$. 对应的等价类称为共轭类：

$$K_a = \{gag^{-1} \mid g \in G\}.$$

- 共轭子群：$A, B \leqslant G$，A 与 B 共轭$\Leftrightarrow \exists\, g \in G$ 使 $gAg^{-1} = B$（或 $g^{-1}Ag = B$）.
- 子群的共轭关系是子群集合$\{H \mid H \leqslant G\}$中的等价关系：A 与 B 共轭$\Leftrightarrow A \sim_c B$. 等价类称为共轭子群类：

$$K_A = \{gAg^{-1} \mid g \in G\}.$$

3. 商群

(1) 正规子群 H 在群中所定义的等价关系：设 $H \triangleleft G$，则 H 在G 中所定义的等价类和商群为

$$a \sim_H b \Leftrightarrow aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH \Leftrightarrow aH \cap bH \neq \varnothing.$$

并称 a 与 b 模 H 同余，记作 $a \equiv b(\mathrm{mod}\ H)$. 其中最常用的条件是

$$a^{-1}b \in H \Leftrightarrow a \equiv b(\mathrm{mod}\ H).$$

当 G 是加群时，有

$$b - a \in H \Leftrightarrow a \equiv b(\mathrm{mod}\ H).$$

形式上与整数集合中的同余关系类似.

等价类：$\bar{a} = aH$.

(2) 商群：$H \lhd G$，则 $G/H = \{aH \mid a \in G\}$ 对子集的运算构成群，称 G/H 为 G 模 H 的商群（商群的记号有时也记作 G/H），它的性质类似于整数模 n 的同余类群 $(Z_n, +)$. 所以我们把商群 G/H 也称为 G 模 H 的同余类群.

4. 正规子群的运算

(1) $A \lhd G, A \leqslant B \Rightarrow A \lhd B$.（但以下命题不成立：$A \lhd B \lhd G \Rightarrow A \lhd G$ 即传递性不成立.）

(2) $A \lhd G, B \lhd G \Rightarrow A \cap B \lhd G, AB \lhd G$.

(3) $A \lhd G, B \leqslant G \Rightarrow A \cap B \lhd B, AB \leqslant G, A \lhd AB$.

（注意比较(2)与(3)的异同.）

(4) $A \lhd G, B \lhd G$ 且 $A \cap B = \{e\} \Rightarrow \forall a \in A, \forall b \in B$ 有 $ab = ba$.（若两个正规子群的交是单位子群，则它们的元素可交换.）

5. 若干重要结果

(1) 指数为 2 的子群必是正规子群.

(2) 若 H 是 G 中惟一的一个阶数为 n 的子群，则 $H \lhd G$.

(3) 正规子群与共轭类的关系：H 是由一些共轭类组成的子群 $\Leftrightarrow H$ 是正规子群.

(4) G 是有限可换群，p 为素数，$p \mid |G| \Rightarrow G$ 中有 p 阶元.（实际上，此定理对有限非可换群 G 亦成立，但以后才能证明.）

(5) **换位子与换位子群**：a 与 b 的换位子是

$$\alpha_{ab} = aba^{-1}b^{-1},$$

a 与 b 可交换的充分必要条件是它们的换位子是单位元：

$$ab = ba \Leftrightarrow \alpha_{ab} = aba^{-1}b^{-1} = e,$$

只有那些不可交换的元素的换位子才不等于单位元. 由 G 中所有换位子生成的子群

$$K = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle$$

称为换位子群，也可定义为 G 中所有换位子的有限乘积所成的集合. 注意不

要理解为所有换位子的集合. K 是 G 的正规子群,且是使对应的商群是可换群的最小子群.(详见后面的习题)

(6) 不含非平凡正规子群的群称为**单群**.

(7) **极大正规子群与单群的关系**: 设 $1<N\lhd G$,如果不存在真包含 N 的非平凡正规子群,则称 N 是极大正规子群. 并有以下定理:

$$N\text{ 是极大正规子群} \Leftrightarrow G/N\text{ 是单群}.$$

该定理在主教材 2.8 节中讲.

二、习题 2.6 详细解答

2.6-1 $A\lhd G,B\lhd G\Rightarrow A\cap B\lhd G,AB\lhd G.$

分析 复习正规子群的概念. 要证明一个子群是正规子群首选的方法是用第(2)个条件检验共轭元是否都在里面.

证 先证第一个结论: $\forall g\in G$ 和 $\forall c\in A\cap B$ 有

$$gcg^{-1}\in A \quad 和 \quad gcg^{-1}\in B,$$

因而 $gcg^{-1}\in A\cap B$,所以 $A\cap B\lhd G$.

再证第二个结论: 首先由 $AB=BA$ 和主教材 2.2 节的子群性质(4)可得 $AB\leqslant G$. 又 $\forall g\in G$ 和 $\forall ab\in AB$ 有

$$gabg^{-1}=gag^{-1}gbg^{-1}=a_1b_1\in AB,$$

所以 $AB\lhd G$.

点评 此题虽然简单,但对于初学者来说应尽量仔细做,这样才能更好理解正规子群的概念,并在运算方面得到一次训练. 其中用到一个前面(参看习题 2.4 第 1 题的点评)已经用过的技巧: 在乘积中间插入 gg^{-1}. 我们把它称为"无中生有"或"插入裂变". 将一个共轭运算裂变为两个共轭运算.

2.6-2 证明 $A\lhd G,B\leqslant G\Rightarrow A\cap B\lhd B,AB\leqslant G.$

分析 本题类似上题,熟悉正规子群的性质.

证 先证 $AB\leqslant G$,与上题相应部分的证明完全相同.

由于 $A\lhd G$,可得 $AB=BA$,从而得到 $AB\leqslant G$.

再证 $A\cap B\lhd B$,注意与上题中相应部分的区别.

$\forall c\in A\cap B,\forall b\in B$,由于 $A\lhd G$,故 $b^{-1}cb\in A$. 另一方面,显然有 $b^{-1}cb\in B$. 所以 $b^{-1}cb\in A\cap B$,故 $A\cap B\lhd B$. 证毕.

2.6-3 设 $H\leqslant G$,则$\{aH\mid a\in G\}$关于子集乘法构成群$\Rightarrow H\lhd G$.

分析 我们已经知道 $H\lhd G\Rightarrow\{aH\mid a\in G\}$关于子集乘法成群. 现在要证逆定理也成立. 要证 $H\lhd G$,我们从正规子群的哪个条件入手呢?

证 方法 1 我们按常规从共轭元下手.

由于$\{aH|a\in G\}$关于子集乘法成群，那么可以看出其中的单位元为H，aH的逆元是$a^{-1}H$：

$(aH)(a^{-1}H)=H\Rightarrow aHa^{-1}H=H.$

因而得$aha^{-1}\in H$，所以$H\lhd G$.

方法2 由于已知条件$\{aH|a\in G\}$关于子集乘法成群给出了集合运算，因而可用共轭子群条件来做：

因为$(aH)(a^{-1}H)=H\Rightarrow aHa^{-1}H=H$，可得$aHa^{-1}\subseteq H$，所以

$$H\lhd G.$$

点评 这两个方法实质上区别不大.

2.6-4 证明四元数群的每一个子群均为正规子群.

分析 复习四元数群(主教材习题2.1第2题)

$$Q_8=\{\pm E,\pm I,\pm J,\pm K\},\quad E=\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad I=\begin{bmatrix}0&-1\\1&0\end{bmatrix},$$

$$J=\begin{bmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{bmatrix},\quad K=\begin{bmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{bmatrix}.$$

可利用群的阶与子群的阶的关系(Lagrange定理)找出所有的子群的阶数，有些直接可以从阶数判断是否是正规子群，必要时找出子群来分析.

证 由于$|Q_8|=8$，它的非平凡子群的阶只能是2或4.

当子群的阶是4时，子群的指数是2，故是正规子群.

当子群的阶是2时，只有一个子群：

$$H=\{E,-E\},$$

显然也是正规子群.

点评 对于低阶群，判断其子群是不是正规子群的问题比较容易.

2.6-5 $A,B\leqslant G,C=\langle A\cup B\rangle$且$B\lhd C$，则$C=AB$.

分析 如果A,B中有一个是G的正规子群，则由正规子群的性质，显然有$C=AB$.但现在给出的条件要弱一些，所以需要详加证明.证明的方法是分析C中元素的形式.

证 首先显然有$AB\subseteq C$.

反之，$\forall c\in C$，c可表示为$c=a_1b_1a_2b_2\cdots$(或$c=b_1a_1b_2\cdots$)，由于$B\lhd C$，$\forall a\in A$有$Ba=aB$，因而$\forall b\in B$有$ba=a\beta,\beta\in B$.所以c可表示为

$$c=a_1b_1a_2b_2\cdots=uv(u\in A,v\in B)\in AB,$$

于是得$C\subseteq AB$.

综上，得证.

点评 本题再次复习生成群的概念和元素的表达方式.

2.6-6 换位子群 $K=\{$换位子的有限乘积$\}$,证明:

(1) $K\lhd G$;

(2) G/K 是可换群;

(3) 若 $N\lhd G$ 且 G/N 可换,则 $N\geqslant K$.

分析 这是一个很重要的定理,首先要把内容搞清. a 与 b 的换位子是

$$\alpha_{ab}=aba^{-1}b^{-1},$$

如果 a 与 b 可交换,则它们的换位子是单位元,只有那些不可交换元素的换位子才不等于单位元. 由所有元素的换位子生成的子群称为**换位子群**,是 G 的正规子群. G 模换位子群所得的商群是可交换群. 而且换位子群具有最小性: 如果另外有一个正规子群对应的商群也可换,则它必然包含换位子群.

我们用语言把问题解释清楚,有利于记忆和直观地理解此定理. 至于证明方法是常规的方法.

证 生成子群的定义,K 可表示为

$$K=\langle\alpha_{ab}\mid a,b\in G\rangle=\{G\text{ 中换位子的有限乘积}\}.$$

(1) 先把 K 的元素表达出来,$\forall x\in K$ 可表示为

$$x=\alpha_{a_1b_1}\alpha_{a_2b_2}\cdots\alpha_{a_kb_k}.$$

为了进行共轭运算,我们先对换位子作共轭运算,利用"无中生有"的伎俩,$\forall g\in G$ 有

$$\begin{aligned}g\alpha_{ab}g^{-1}&=gaba^{-1}b^{-1}g^{-1}=gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1}\\&=gag^{-1}gbg^{-1}(gag^{-1})^{-1}(gbg^{-1})^{-1}=\alpha_{g(a)g(b)}.\end{aligned}$$

其中记 $g(a)=gag^{-1}$,由 g 所确定的共轭变换. 则

$$\begin{aligned}g(x)&=gxg^{-1}=g(\alpha_{a_1b_1}\alpha_{a_2b_2}\cdots\alpha_{a_kb_k})g^{-1}=g(\alpha_{a_1b_1})g(\alpha_{a_2b_2})\cdots g(\alpha_{a_kb_k})\\&=\alpha_{g(a_1)g(b_1)}\alpha_{g(a_2)g(b_2)}\cdots\alpha_{g(a_k)g(b_k)}\in K,\end{aligned}$$

所以 $K\lhd G$.

(2) 要证商群 G/K 是可换群,可用商群中的换位子来证明:

$$\forall aK,\quad bK\in G/K,\quad (aK)(bK)(aK)^{-1}(bK)^{-1}=aba^{-1}b^{-1}K=K,$$

因而$(aK)(bK)=(bK)(aK)$,所以 G/K 是可换群.

(3) 设 $N\lhd G$ 且 G/N 可换,即$(aN)(bN)(aN)^{-1}(bN)^{-1}=aba^{-1}b^{-1}N=N$,于是有 $aba^{-1}b^{-1}\in N$.

所以 $K=\langle aba^{-1}b^{-1}\mid a,b\in G\rangle\leqslant N$.

点评 本题的目的是对换位子群的性质有所了解、本题结论(2)说明换位子群的商群是可交换的,形象地说,一个不可交换群模(抹)掉换位子群就变成可交换了,其实并不是同一个群. 本题结论(3)说明换位子群是使其商群可交

换的最小正规子群.

2.6-7 证明一个可换群如果是单群,则它必是素数阶循环群.

分析 复习单群的定义.我们可从群的阶或从元素的阶入手,分无限群和有限群两种情况来讨论.下面就用两种方法来证明此题.

证 **方法1** 分无限群和有限群两种情况.

(1) $|G|=\infty$,任取 $a\in G\setminus\{e\}$.

若 $o(a)=m$,则 $m>1$ 和 $1<\langle a\rangle\lhd G$,与 G 是单群矛盾,故必有 $o(a)=\infty$.若$\langle a\rangle<G$,则 $1<\langle a\rangle\lhd G$,与 G 是单群矛盾,所以只有$\langle a\rangle=G$,即 G 是循环群.(这里用1代表单位子群.1经常用来代表单位元,或单位子群等,根据不同的场合,心照不宣.)循环群是可交换群,它的任何子群都是正规子群,于是有 $1<\langle a^2\rangle\lhd G$,与 G 是单群矛盾.这就证明了无限群不是单群.

(2) $|G|=n$,若 n 为合数,必有素数 $p<n$ 和 $p\mid n$,由主教材定理2.6.3,G 中有 p 阶元 a,因而有 $1<\langle a\rangle\lhd G$,与 G 是单群矛盾.所以必有

$$|G| = n = \text{素数}.$$

我们熟知素数阶群是循环群(主教材定理2.5.2推论(3)),所以 G 是素数阶循环群.

方法2 从元素的阶入手,请读者自己完成.

点评 这两个方法类似,似乎方法二更简单一些.

2.6-8 A_4 是否是单群?

分析 如果是肯定的回答,就要证明;如果是否定的回答,则只需找一个非平凡正规子群.

解 否!因为我们很容易在 A_4 中找到一个正规子群:

$$1 < K_4 = \{(1),(12)(34),(13)(24),(14)(23)\}\lhd A_4.$$

所以 A_4 不是单群.

点评 这是 A_n 中最大的非单群,下一节要证明 $A_n(n\geqslant 5)$都是单群.

***2.6-9** $|G|=2n$,且 n 是奇数,则存在 $H\lhd G$ 且$[G:H]=2$.

分析 实际上只需证明存在指数为2的子群就可以了.因为指数为2的子群必为正规子群(主教材例2.6.1),而指数为2的子群就是元素个数占一半的子群.联想到置换群的一个性质:要不全是偶置换,要不奇偶置换各半.当群中有奇置换时,那一半的偶置换就构成指数为2的子群.因此问题归结为要证明群中存在奇置换就可.但是 G 不一定是置换群,利用Cayley定理,可将 G 同构于一个置换群.

我们首先找出与 G 同构的置换群.由Cayley定理,G 同构于下面的置换群:

$$G' = \{\sigma_a \mid a \in G, \sigma_a(x) = ax\}.$$

下面我们要证 G'中有奇置换. 为此，再看一下已知条件$|G|=2n$，回忆一下前面涉及偶数阶群的性质(习题2.2-5)：偶数阶群必有二阶元. 二阶元是否是奇置换呢？不一定. 因为在置换群中二阶元可表示为一些不相交的对换的乘积，而这个二阶元的奇偶性由乘积所含的对换个数的奇偶性所决定. 例如二阶元 $\tau=(12)$是奇置换，但二阶元 $\tau_1=(12)(34)$是偶置换. 为此，再看一下已知条件：$|G'|=|G|=2n$ 且 n 是奇数，设 σ_b 是 G'中的一个二阶元，我们将 σ_b 表达出来：首先 σ_b 是一些不相交的对换的乘积；其次由于 $\sigma_b=bx$, $\forall x\in G$，是一个所谓“左平移”变换，在 G 上没有不动点，即不含长度为 1 的轮换. 由以上两点，设 $G=\{1,2,\cdots,2n\}$，则 σ_b 可表示为：

$$\sigma_b = (i_1, j_1)(i_2, j_2)\cdots(i_n, j_n).$$

由于 n 是奇数，所以 σ_b 是奇置换.

这样问题就证明了. 但要简洁地把证明书写出来，于是用尽量少的文字表达如下.

证 由 Cayley 定理，G 同构于下面的置换群：

$$G' = \{\sigma_a \mid a \in G, \sigma_a(x) = ax\}.$$

由$|G'|=|G|=2n$，G'中必有一个二阶元，设为 σ_b，它可表示为一些不相交的对换的乘积.

因为 $\sigma_b(x)=bx$, $\forall x\in G$，是一个没有不动点的置换. 设 $G=\{1,2,\cdots,2n\}$，则 σ_b 可表示为

$$\sigma_b = (i_1, j_1)(i_2, j_2)\cdots(i_n, j_n).$$

由于 n 是奇数，所以 σ_b 是奇置换. 因而 G'中奇偶置换各占一半，于是令 H'为 G'中所有偶置换构成的子群，则$[G':H']=2$ 和 $H'\lhd G'$. 设 G 中与 H'对应的子群为 H，则$[G:H]=2$ 和 $H\lhd G$. 证毕.

点评 该题涉及的内容比较多，对初学者来说难度比较大.

2.7 共轭元和共轭子群

一、内容提要

1. 中心和中心化子

- **群的中心**：和群中所有元素都可交换的元素集合构成群的中心，是一个正规子群. 用式子表达：

$$C(G) = \{a \mid \forall x \in G: ax = xa\}.$$

并有 $C(G)\lhd G$ 和 $C(G)=G\Leftrightarrow G$ 是 Abel 群.

- **中心化子**：一个元素的中心化子是与此元素可交换的所有元素构成的集合，是一个子群，用式子表达：

$$a\in G \text{ 的中心化子}：C_G(a)=\{g\in G\mid ga=ag\}.$$

一个子集的中心化子是与此子集的元素都可交换的所有元素构成的集合，是一个子群，用式子表达：

$$S\subseteq G \text{ 中心化子}：C_G(S)=\{g\in G\mid \forall x\in S:gx=xg\}.$$

- **性质**：$\langle a\rangle\leqslant C_G(a)\leqslant G.\ C(G)\lhd C_G(a)\leqslant G.$

注意：记号比较复杂，不要搞混！

2. 共轭元和共轭类（概念前面已经介绍过）

- a 与 b 共轭：$\exists g\in G$ 使 $gag^{-1}=b$（或 $g^{-1}ag=b$）.
- 以 a 为代表的共轭元素类：$K_a=\bar{a}=\{gag^{-1}\mid g\in G\}$. 中心里的每个元素自成一个共轭类：$a\in C(G)\Leftrightarrow K_a=\{a\}$.
- **共轭类基数定理**：一个共轭类中元素的个数：$|K_a|=|\{gag^{-1}\mid g\in G\}|=[G:C_G(a)]$.
- **类方程**（按共轭类分类计算群的元素个数）：

$$|G|=|C|+\sum_{a\notin C}|K_a|=|C|+\sum_{a\notin C}[G:C_G(a)],$$

其中和式只对非中心元素的共轭类的代表元求和. 此公式很有用.

- **正规子群与共轭元素类的关系**：正规子群由一些共轭元素类的并构成，反之，如果一些共轭元素类的并构成一个群，则此群是正规子群.

这就为确定所有正规子群提供了一个方法：先求出所有共轭元素类，看哪些共轭元素类的并能构成群，由此可得到全部的正规子群.

3. 共轭子群和共轭子群类（注意这个概念与共轭元和共轭元素类相应概念与公式的类似）

- 两子群 H 与 K 共轭：$\exists g\in G$ 使 $gHg^{-1}=K$（或 $g^{-1}Hg=K$）.
- 以子群 H 为代表的共轭子群类：$K_H=\bar{H}=\{gHg^{-1}\mid g\in G\}$.
- 子群 H 的正规化子：$N_G(H)=\{g\in G\mid gHg^{-1}=H\}$. 用语言来表达：$H$ 的正规化子就是对 H 作共轭运算而保持 H 不变的所有元素. 且有 $H\lhd N_G(H)\leqslant G$. 正规子群的正规化子就是整个群.
- **正规化子的性质**：若有 K 使 $H\lhd K\leqslant G$，则 $K\leqslant N_G(H)$（正规化子的最大性：非正规子群 H 的正规化子就是包含 H 作为正规子群的最大子群.）. 显然有 $H\lhd G\Leftrightarrow N_G(H)=G$.

- **共轭子群类基数定理**：以 H 为代表的共轭子群类中的子群个数与正规化子有关：$|K_H|=[G:N_G(H)]$.
- 子群数目计算公式：与类方程类似，可得一个群内子群数目的计算公式. 设 S 是群 G 的所有子群的集合，N 是群 G 的所有正规子群的集合，则

$$|S|=|N|+\sum_{H\notin N}|K_H|=|N|+\sum_{H\notin N}[G:N_G(H)],$$

  其中和式只对非正规子群的共轭类的代表元求和.

此式虽然给出了求群内子群数目的计算方法，但实际使用并不方便.

4. 若干结果

(1) 设 p 为素数，$|G|=p^n$，称 G 为 p-群. 则 p-群有非平凡中心，而且有 p 阶元.

(2) 至此，我们可以证明一般的 Cauchy 定理：G 是有限群，p 为素数，$p\mid|G|$，则G 中有 p 阶元. 因而有 p 阶子群.

证 对$|G|$作归纳法. $|G|=p$ 显然成立，下设$|G|>p$.

如果 G 是可换群，定理已证. 因而下设 G 不是可换群.

如果存在 $a\in G\backslash C(G)$，满足 $p\mid|C_G(a)|$，则因为$|C_G(a)|<|G|$，由归纳假设，$C_G(a)$中有 p 阶元. 得证.

否则，$\forall a\in G\backslash C(G)$均有 $p\nmid|C_G(a)|$，因而由拉格朗日定理得 $p\mid[G:C_G(a)]$. 考虑类方程：

$$|G|=|C|+\sum_{a\notin C}|K_a|=|C|+\sum_{a\notin C}[G:C_G(a)],$$

得到 $p\mid|C(G)|$. 由于定理对可换群成立，所以 $C(G)$中有 p 阶元.

证毕.

(3) **S_n 中的共轭类**：S_n 中两元素共轭的充分必要条件是它们的类型相同. 每类的元素数目见习题 2.7-7，由此得 S_n 中共轭类的类数是方程

$$1\cdot\lambda_1+2\cdot\lambda_2+\cdots+n\cdot\lambda_n=n$$

的非负整数解的个数.

(4) **A_n 中的共轭类**：情况比较复杂. 设 $\sigma\in A_n$，令 K_σ 为所有与 σ 同类型的置换的集合，则 K_σ 在 A_n 中是否是同一共轭类还要看 $C_{S_n}(\sigma)$是否包含奇置换：当 $C_{S_n}(\sigma)$包含奇置换时，K_σ 在 A_n 中是一个共轭类；当 $C_{S_n}(\sigma)$不包含奇置换时，K_σ 在 A_n 中是两个共轭类：

$K'_\sigma=\{\tau\sigma\tau^{-1}\mid\tau\in S_n$ 且 τ 是偶置换$\}$，$K''_\sigma=\{\tau\sigma\tau^{-1}\mid\tau\in S_n$ 且 τ 是奇置换$\}$.

(5) **$A_n(n\geqslant5)$是单群**. 其证明方法技巧性很高：首先从这样一个事实出

发，任何一个置换群中，有最多的不动点数的非单位元素中必有形式为 $1^r p^s$-型的元素，其中 p 为素数. 然后证明 A_n 中的任何非单位正规子群包含所有的 3 轮换.

二、习题 2.7 详细解答

2.7-1 $G=GL_2(\mathbb{C})$，$N=\left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\middle| ad\neq 0\right\}$，$H=\left\{\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}\middle| t\in C\right\}$. 求 $C(G)$，$C_G(N)$，$C_N(H)$，$N_G(H)$.

分析 先看懂符号，对初学者来说，不妨对照内容提要，把每一个量的定义写出来，按照定义来做.

解 (1) 求中心 $C(G)$. 由线性代数中的结果：与所有矩阵均可交换的矩阵是数量矩阵(参看第 1 章补充题-3)，知

$$C(G)=\{\alpha I \mid \alpha\in C^*\}.$$

(2) 求 N 在 G 中的中心化子 $C_G(N)$，按定义应为

$$C_G(N)=\{A\in G \mid \forall B\in N: AB=BA\},$$

用待定系数法：设

$$A=\begin{bmatrix}x & y\\ w & z\end{bmatrix},\quad B=\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}.$$

由 $AB=BA$ 得方程组：

$$\begin{aligned}ax &= ax+bw,\\ xb+yd &= ay+bz,\\ aw &= dw,\\ bw+dz &= dz.\end{aligned}$$

得 $bw=0$，$(a-d)w=0$，$b(x-z)=(a-d)y$.

由于 b 可取任意非 0 元素，所以有 $w=0$；由于 b 也可取 0，a,d 可取不同复数，所以有 $y=0$；因而得 $x=z$.

综上得 $C_G(N)=\{\alpha I\mid\alpha\in C^*\}=C(G)$.

(3) 求 H 在 N 中的中心化子 $C_N(H)$，按定义应为

$$C_N(H)=\{B\in N \mid \forall C\in H: BC=CB\},$$

用待定系数法：设

$$C=\begin{bmatrix}1 & t\\ 0 & 1\end{bmatrix},\quad B=\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}.$$

由 $CB=BC$ 得方程组：

$$b+td=at+b,$$

得$(a-d)t=0$. 由于 t 可取任意复数,故 $a=d$. 所以

$$C_N(H)=\left\{\begin{bmatrix}a & b\\ 0 & a\end{bmatrix} \mid a,b\in C, a\neq 0\right\}.$$

(4) 求 H 在 G 中的正规化子 $N_G(H)$,按定义

$$N_G(H)=\{g\in G\mid gHg^{-1}=H\}.$$

$$\begin{aligned}gHg^{-1}&=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\left\{\begin{bmatrix}1 & t\\ 0 & 1\end{bmatrix}\middle| t\in C\right\}\begin{bmatrix}a & b\\ c & d\end{bmatrix}^{-1}\\ &=\left\{\frac{1}{ad-bc}\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & t\\ 0 & 1\end{bmatrix}\begin{bmatrix}d & -b\\ -c & a\end{bmatrix}\middle| t\in C\right\}\\ &=\left\{\frac{1}{ad-bc}\begin{bmatrix}ad-bc-act & a^2t\\ -c^2t & ad-bc\end{bmatrix}\middle| t\in C\right\}\\ &=H=\left\{\begin{bmatrix}1 & t\\ 0 & 1\end{bmatrix}\mid t\in C\right\},\end{aligned}$$

故得 $c=0$,所以

$$N_G(H)=\left\{\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}\mid ad\neq 0, b\in C\right\}=N.$$

点评 要根据定义仔细算. 通过计算熟悉中心、中心化子和正规化子等概念,可以在置换群中作类似的题,例如 $G=S_4$, $\sigma=(12)$, $H=\langle(12)\rangle$,求 $C(G)$, $C_G(H)$, $N_G(H)$.

2.7-2 设 $H\leqslant G$,证明:

(1) $C_G(H)\lhd N_G(H)$;

(2) $C_G(C_G(C_G(H)))=C_G(H)$.

分析 由于符号比较复杂,我们必须小心地从定义出发. 凡是我们初学的东西,还不熟悉的时候,最基本的方法是"从定义出发",然后到基本定理,最后才想想有什么技巧、高招. 这个过程实际上是一个复习的过程,是做题的真正目的.

证 (1)先把定义写出来:

$C_G(H)=\{a\in G\mid \forall h\in H: ah=ha\}$

(与 H 的每一个元素可交换的元素集合),

$N_G(H)=\{g\in G\mid gHg^{-1}=H\}=\{g\in G\mid gH=Hg\}$

(与 H 可交换的元素集合),

显然,与 H 的每一个元素可交换的元素自然与 H 可交换,因而 $C_G(H)\leqslant N_G(H)$. 再根据正规子群的条件, $\forall a\in C_G(G)$, $\forall g\in N_G(G)$,看 gag^{-1} 是否在 $C_G(H)$ 里,也就是 gag^{-1} 是否与 H 中的元素都可交换? 我们用换位子

$(gag^{-1})h(gag^{-1})^{-1}h^{-1}$来做,由于 $g^{-1}hg\in H$,可令 $g^{-1}hg=h_1$,于是

$$(gag^{-1})h(gag^{-1})^{-1}h^{-1}=gah_1a^{-1}g^{-1}h^{-1}=gh_1g^{-1}h^{-1}=hh^{-1}=e,$$

所以 $gag^{-1}\in C_G(H)$,$C_G(H)\lhd N_G(H)$.

(2) 由于 $C_G(H)=\{a\in G\mid \forall h\in H:ah=ha\}$,$H$ 中的元素与 $C_G(H)$中的元素都可交换,因而

$$H\leqslant C_G(C_G(H)). \tag{$*$}$$

一方面,易见:$H\leqslant K\Rightarrow C_G(H)\geqslant C_G(K)$(这是因为与 K 中元素都可交换的元素必然与 H 中元素都可交换).所以

$$C_G(H)\geqslant C_G(C_G(C_G(H))).$$

另一方面,在式($*$)中用 $C_G(H)$代替 H,得

$$C_G(H)\leqslant C_G(C_G(C_G(H))).$$

综上得证.

点评 由以上证明过程,我们得到关于中心化子的两个副产品:设 H,$K\leqslant G$,则有

$$H\leqslant C_G(C_G(H)),$$
$$H\leqslant K\Rightarrow C_G(H)\geqslant C_G(K).$$

2.7-3 设$|G|<\infty$,$H<G$,G 中与 H 共轭的全部子群为 $H_1,H_2,\cdots,H_k$,则 $\bigcup_{i=1}^{k}H_i$是 G 的真子集.

分析 解读:G 是有限群,H 是 G 的真包含的子群,要证 H 的全部共轭子群的并是 G 的真包含子集.因为涉及全部共轭子群,可利用共轭子群类基数定理来证.

证 当 $k=1$ 时显然成立.

下面设 $k\geqslant 2$.考虑到所有子群都含单位元,因而

$$\left|\bigcup_{i=1}^{k}H_i\right|\leqslant\sum_{i=1}^{k}|H_i|-(k-1),$$

由共轭子群类基数定理,$k=|K_H|=[G:N_G(H)]$,得

$$\left|\bigcup_{i=1}^{k}H_i\right|\leqslant\sum_{i=1}^{k}|H_i|-(k-1)=k|H|-(k-1)$$
$$=[G:N_G(H)]\cdot|H|-(k-1),$$

由于 G 是有限群,$H\leqslant N_G(H)$,和 Lagrange 定理,有

$$\left|\bigcup_{i=1}^{k}H_i\right|\leqslant\frac{|G|}{|N_G(H)|}\cdot|H|-(k-1)$$
$$\leqslant|G|-(k-1)<|G|.$$

所以 $\bigcup_{i=1}^{k} H_i$ 是 G 的真子集.

点评 该题涉及许多内容,要认真思考.

2.7-4 设 $|G|=p^2$(p 是素数),则 G 是可换群.

分析 表面上看起来似乎与群 $|G|=p$ 只差一步之遥,但实际并不简单.首先可能会从元素的阶去考虑,但并不很快能解决.于是我们从中心来考虑:$C(G)=G \Leftrightarrow G$ 是 Abel 群.

证 由于 p-群有非平凡中心,故 $1<C(G)\leqslant G$.

如果 $C(G)<G$,则 $|C(G)|=p$.取 $a\in G\backslash C(G)$,则 $C(G)<C_G(a)\leqslant G$,因而由 Lagrange 定理有 $|C_G(a)|\,|\,|G|$,且因 $|C_G(a)|>p$,所以 $|C_G(a)|=p^2$,从而得到 $C_G(a)=G, a\in C(G)$,与 $a\in G\backslash C(G)$ 矛盾.

所以 $C(G)=G$, G 是可换群.

点评 类似的方法可证明以下问题:设 $|G|=p^3$(p 是素数),且 G 不是可换群,则有 $|C(G)|=p$.请读者自己完成证明.

2.7-5 $|G|=pq$, p,q 为互异素数,且 $p<q$,则 G 中的 q 阶子群是正规子群.

分析 与上一题类似,可能会从元素的阶来考虑,但往前走,困难较大.于是我们从要证明的结论下手,要证明 q 阶子群是正规子群,即要证明它是自共轭子群,不妨从反面考虑,如果 q 阶子群不是正规子群,那会怎样?

证 设 H 是 G 中的一个 q 阶子群,要证它是正规子群.

用反证法.假设 H 不是正规子群,则存在 $g\in G$ 使 $gHg^{-1}\neq H$.由于 $|gHg^{-1}|=|H|=q$, $(gHg^{-1}\cap H)<H$, $|gHg^{-1}\cap H|\,|\,q$,得 $|gHg^{-1}\cap H|=1$.于是由子群乘积的基数公式(定理 2.5.3)有

$$|gHg^{-1}H|=\frac{|gHg^{-1}|\cdot|H|}{|gHg^{-1}\cap H|}=q^2>pq,$$

与 $gHg^{-1}H\subseteq G$ 矛盾.

所以 H 是正规子群.

点评 以上的证明方法已经很简单了.如果从元素的阶出发,不会有这样简单,所以不必再浪费时间.

2.7-6 设 $|G|=p^n$(p 是素数),则 G 中非正规子群的个数是 p 的倍数.

分析 这个问题的关键是搞清"非正规子群"的意义,把它与共轭子群和共轭子群类联系起来:H 是非正规子群 $\Leftrightarrow \exists g\in G: gHg^{-1}\neq H \Leftrightarrow |K_H|=|\{gHg^{-1}\mid g\in G\}|>1$.因此基数大于 1 的共轭子群类中的子群都是非正规子群,由此可求出全部非正规子群的个数了.

证　对于不存在非正规子群的情况，0也是 p 的倍数. 结论成立. 下面设 G 中存在非正规子群.

设 H 是任一非正规子群，则共轭子群类 $K_H=\{gHg^{-1}\mid g\in G\}$ 中的子群都不是正规子群，其个数为 $|K_H|=|\{gHg^{-1}\mid g\in G\}|>1$，由共轭子群类基数定理得

$$|K_H|=[G:N_G(H)]=\frac{|G|}{|N_G(H)|}=\frac{p^n}{|N_G(H)|}.$$

因此，$|K_H|=p^\alpha,\alpha>0$.

由于 G 中全部非正规子群的个数为

$$m=\sum_{\substack{H\leqslant G\\ \text{且}H\text{非正规}}}|K_H|,$$

其中和式是对非正规子群的共轭子群类的代表元求和.

因为 p 能整除和式中的每一项，所以

$$p\mid m.$$

点评　该题还提供了以下的公式：

G 的全部非正规子群的数目为 $\sum\limits_{\substack{H\leqslant G\\ \text{且}H\text{非正规}}}|K_H|$，其中和式是对非正规子群的共轭类代表元求和.

G 的全部子群的数目为 $\sum\limits_{H\leqslant G}|K_H|$，其中和式是对子群的共轭类代表元求和，详见本节提要中有关内容.

2.7-7　证明在 S_n 中 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$-型置换的个数为 $\dfrac{n!}{1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\lambda_1!\ \lambda_2!\ \cdots\lambda_n!}$.

分析　先把 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$-型置换表达出来，然后与全排列相联系.

证　设 σ 是一个 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$-型置换，可表示为以下形式：

$$\sigma=\underbrace{(*)\cdots(*)}_{\lambda_1}\underbrace{(*\ *)\cdots(*\ *)}_{\lambda_2}\cdots\underbrace{(*\ *\cdots *)}_{\lambda_n}.$$

把任何一个 n 元排列放入括号内，就形成一个置换，由于有 $n!$ 个全排列，这样可形成 $n!$ 个置换，但这些置换有些是相同的.

首先，在每一个长度为 k 的轮换中，与哪一个元素打头无关，因而有 k 种选择. 共有 λ_k 个长度为 k 的轮换，因此应除以 k^{λ_k}，$k=1,2,\cdots,n$.

再看 λ_k 个长度为 k 的轮换，它们的 $\lambda_k!$ 个不同次序对应的是同一个置换，因此应除以 $\lambda_k!$，$k=1,2,\cdots,n$.

综上，公式成立.

点评　该题的证明关键之处在于对置换的表示方法的理解. 方法实际上

是初等的.

2.7-8 确定 A_4 中的共轭类与正规子群.

分析 先复习关于 A_n 的共轭类的定理 2.7.6. 然后选取代表元,根据它的类型,写出所有同类型的元素. 再根据定理 2.7.6 来确定这些同类型的元素是同一个共轭类呢还是分裂为两个共轭类.

有了共轭类后,看哪些共轭类的并能形成群,则得到正规子群.

解 我们按元素的阶由小到大来分析.

一阶元: $K_1=\{(1)\}$.

二阶元: 取 $\tau=(1,2)(3,4))$,由于$(12)\in C_{S_4}(\tau)$,含奇置换,由定理 2.7.6,只有以下一个共轭类:

$$K_\tau=\{(12)(34),(13)(24),(14)(23)\}.$$

三阶元: 取 $\sigma=(1,2,3)$,由于 $C_{S_4}(\sigma)=\{(1),(123),(132)\}$,不含奇置换,由定理 2.7.6,有以下两个共轭类:

$$K_\sigma^{(1)}=\{(123),(134),(243),(142)\},$$
$$K_\sigma^{(2)}=\{(132),(234),(143),(124)\}.$$

A_4 中的正规子群由共轭类组成,有

$$H_1=\{(1)\},$$
$$H_2=\{(1),(12)(34),(13)(24),(14)(23)\},$$
$$H_3=A_4.$$

点评 读者如有时间不妨求一下 A_5 中的共轭类和正规子群.

2.7-9 确定二面体群 D_6 的共轭类与正规子群.

分析 首先,对二面体群有个表示方法问题,我们现在至少有三种表示方法: 几何表示法,抽象表示法和置换表示法. 我们采用哪一种表示方法呢?

由于我们对置换群的共轭类讨论较多,不妨采用置换表示法.

解 首先,对二面体群用置换表示法写出来:

$$\begin{aligned}D_6=\{&(1),(123456),(135)(246),(14)(25)(36),(153)(264),\\&(165432),(26)(35),(12)(36)(45),(13)(46),\\&(14)(23)(56),(15)(24),(16)(25)(34)\}.\end{aligned}$$

现在我们只能说: 两元素共轭,则类型相同. 但反过来不对. 所以我们只能在同类型的置换中分析是一个共轭类还是几个共轭类.

1^6 型元素即单位元,自成一个共轭类: $K_1=\{(1)\}$.

6^1 型元素构成一个共轭类: $K_2=\{(123456),(165432)\}$,因为取 $\tau=(26)(35)$,则$\tau(123456)\tau^{-1}=(165432)$.

3^2 型元素构成一个共轭类: $K_3=\{(135)(246),(153)(264)\}$,取 $\tau=$

(26)(35)，则$\tau(135)(246)\tau^{-1}=(153)(264)$.

$1^2 2^2$ 型元素构成一个共轭类：设 $\sigma=(26)(35)$，取 $\tau_1=(123456)$，则 $\tau_1(26)(35)\tau_1^{-1}=(31)(46)$. 取 $\tau_2=(165432)$，则 $\tau_2(26)(35)\tau_2^{-1}=(15)(24)$. 所以得到

$$K_4=\{(26)(35),(13)(46),(15)(24)\}.$$

2^3 型元素构成 2 个共轭类：

设 $\sigma=(14)(25)(36)$，经过运算发现它与其他元素都可交换，所以 $\sigma\in C(D_6)$，自成一个共轭类：

$$K_5=\{(14)(25)(36)\}.$$

设 $\sigma=(12)(36)(45)$，取 $\tau_1=(123456)$，则 $\tau_1(12)(36)(45)\tau_1^{-1}=(23)(14)(56)$. 取 $\tau_2=(165432)$，则 $\tau_2(12)(36)(45)\tau_2^{-1}=(16)(25)(34)$. 所以

$$K_6=\{(12)(36)(45),(14)(23)(56),(16)(25)(34)\}.$$

综上，共有 6 个共轭类.

正规子群有

$H_1=\{(1)\}$,

$H_2=C(D_6)=\{(1),(14)(25)(36)\}$,

$H_3=K_1\cup K_3=\{(1),(135)(246),(153)(264)\}$,

$H_4=K_1\cup K_2\cup K_3=\langle(123456)\rangle=C_6$,

$H_5=K_1\cup K_3\cup K_4$

$\quad=\{(1),(135)(246),(153)(264)\}\cup\{(26)(35),(13)(46),(15)(24)\}$,

$H_6=D_6$.

点评 以上的方法虽然元素很具体，但这种方法只能具体问题具体分析，不能得到一般的结论. 如果我们用一般形式，则可得到一般的公式.

二面体群的抽象表示形式为

$D_n=\{a^i,a^ib\mid i=0,1,\cdots,n-1;o(a)=n,o(b)=2,ba=a^{-1}b\}$.

先考虑$\langle a\rangle$中的共轭类. 由于 $ba^ib^{-1}=a^{-i}$，所以$\langle a\rangle$中的共轭类有

$$L_i=\{a^i,a^{n-i}\},\quad i=0,1,\cdots,\left\lfloor\frac{n}{2}\right\rfloor.\quad \lfloor x\rfloor\text{表示 } x \text{ 的下整数}.$$

得到共$\left\lfloor\frac{n}{2}\right\rfloor+1$ 个共轭类.

再考虑 $D_n\setminus\langle a\rangle$ 中的共轭类：由于 $a^k(a^ib)a^{-k}=a^{2k+i}b$，故 $a^ib\sim a^{2k+i}b$. 所以

当 $n\equiv0\pmod 2$时得到以下两个共轭类：

$$K_1 = \left\{ a^{2k}b \,\middle|\, k = 0,1,\cdots,\frac{n}{2}-1 \right\},$$

$$K_2 = \left\{ a^{2k+1}b \,\middle|\, k = 0,1,\cdots,\frac{n}{2}-1 \right\}.$$

综上，共得到$\left\lfloor \frac{n}{2} \right\rfloor+3$ 个共轭类.

当 $n\equiv 1 \pmod 2$时得到以下一个共轭类：

$$K_1 = \{a^k b \mid k = 0,1,\cdots,n-1\}.$$

综上，共得到$\left\lfloor \frac{n}{2} \right\rfloor+2$ 个共轭类.

下面分析有哪些正规子群.

首先 $C_n=\langle a\rangle$及其子群都是正规子群，它们是

$$N_d = \langle a^d \rangle, \quad d \mid n.$$

其次，当 $n\equiv 0 \pmod 2$时有以下的正规子群：

$$L = \left\{ a^{2k}, a^{2k}b \,\middle|\, k = 0,1,\cdots,\frac{n}{2}-1 \right\}.$$

* **2.7-10** 设 $G=\left\{ \begin{bmatrix} 1 & 0 \\ a & \varepsilon \end{bmatrix} \,\middle|\, \varepsilon = \pm 1, a\in\mathbb{Z} \right\}$是对矩阵乘法构成的群，确定 G 的全部共轭类和正规子群.

分析 矩阵群中的共轭就是相似，要具体进行计算.

解 作相似运算：取 $A=\begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}$，对任意 $g=\begin{bmatrix} 1 & 0 \\ n & \varepsilon \end{bmatrix}\in G$，计算

$$gAg^{-1} = \begin{bmatrix} 1 & 0 \\ n & \varepsilon \end{bmatrix}\begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -\varepsilon n & \varepsilon \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \varepsilon a & 1 \end{bmatrix},$$

得共轭类

$$K_a = \overline{\begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}} = \left\{ \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -a & 1 \end{bmatrix} \right\}, \quad a = 0,1,2,\cdots.$$

取 $B=\begin{bmatrix} 1 & 0 \\ a & -1 \end{bmatrix}$，对任意 $g=\begin{bmatrix} 1 & 0 \\ n & \varepsilon \end{bmatrix}\in G$，计算

$$gBg^{-1} = \begin{bmatrix} 1 & 0 \\ n & \varepsilon \end{bmatrix}\begin{bmatrix} 1 & 0 \\ a & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -\varepsilon n & \varepsilon \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2n+\varepsilon a & -1 \end{bmatrix},$$

得共轭类：

$$K' = \overline{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}} = \left\{ \begin{bmatrix} 1 & 0 \\ 2n & -1 \end{bmatrix} \,\middle|\, n \in \mathbb{Z} \right\}.$$

$$K''=\overline{\begin{bmatrix}1 & 0\\ 1 & -1\end{bmatrix}}=\left\{\begin{bmatrix}1 & 0\\ 2n+1 & -1\end{bmatrix}\middle| n\in\mathbb{Z}\right\}.$$

正规子群为

$$H_0=1,$$

$$H_k=\bigcup_{k|a}K_a=\left\{\begin{bmatrix}1 & 0\\ mk & 1\end{bmatrix}\middle| m\in\mathbb{Z}\right\};\quad k=1,2,\cdots.$$

$$N_1=H_0\cup H_2\cup K'=\left\{\begin{bmatrix}1 & 0\\ 2m & 1\end{bmatrix},\begin{bmatrix}1 & 0\\ 2m & -1\end{bmatrix}\middle| m\in\mathbb{Z}\right\}.$$

$$N_2=H_0\cup H_2\cup K''=\left\{\begin{bmatrix}1 & 0\\ 2m & 1\end{bmatrix},\begin{bmatrix}1 & 0\\ 2m+1 & -1\end{bmatrix}\middle| m\in\mathbb{Z}\right\}.$$

点评　在计算过程中要注意哪些量是变的，哪些是暂时固定的，才能准确确定共轭类.

2.8　群的同态

一、内容提要

在前面我们已经对同构比较熟悉，两个群同构，从代数上看而不考虑实际意义，就是这两个群完全相同. 本节所要学习的同态，是指两个群有某种相似性.

1. 群的同态的概念

设$(G,\cdot)$，$(G',\circ)$是两个群，若有映射 $f:G\to G'$满足 $\forall a,b\in G$ 有 $f(a\cdot b)=f(a)\circ f(b)$（这个关系式称为“保持运算”），则称 f 是一个 G 到 G' 的同态(映射).

注意：同态与同构的定义比较，只差一字：在同构的定义中是“双”射，而同态是“映”射，真是差之毫厘，失之千里.

- $f(e)=e'$，$f(a^{-1})=f(a)^{-1}$，(实际上，$f(a^n)=(f(a))^n$，$n\in\mathbb{Z}$).
- $H\leqslant G\Rightarrow f(H)\leqslant G'$，特别是 $f(G)\leqslant G'$；$H\lhd G\Rightarrow f(H)\lhd f(G)$.
- 当 f 是单射，称 f 是单同态，这时 $G\simeq f(G)$.
- 当 f 是满射，称 f 是满同态，这时记作 $G\overset{f}{\sim}G'$.
- 当 f 是双射，则 f 是同构，这时记作 $G\overset{f}{\cong}G'$.
- **同态核**：G' 中的单位元 e' 的全原像称为同态的核，它是 G 的正规子群：

$$\ker f=\{a\in G \mid f(a)=e'\}\lhd G.$$

- f 是单同态$\Leftrightarrow\ker f=1$. $G\overset{f}{\sim}G'$,则 f 是同构$\Leftrightarrow\ker f=1$.
- f 是零同态：$\forall x\in G$ 有 $f(x)=e'$.
- 同态的全原像：
  $f(a)=a'\Rightarrow f^{-1}(a')=a\ker f$. 当 G 是加群时,$f^{-1}(a')=a+\ker f$.
  $f(H)=H'\Rightarrow f^{-1}(H')=H\ker f$. 当 G 是加群时,$f^{-1}(H')=H+\ker f$.
  $H'\leqslant f(G)\Rightarrow f^{-1}(H')\leqslant G$,$H'\lhd f(G)\Rightarrow f^{-1}(H')\lhd G$.

2. 同态的重要例子

- $f: a\mapsto \bar{a}\ (\bmod n)$,$((\mathbb{Z},+)\to(Z_n,+))$. $\ker f=\langle n\rangle$.
- 群到其商群的**自然同态**：设 $H\lhd G$,则 $\varphi: a\mapsto aH\ (G\to G/H)$是同态.

3. 关于同态的定理

(1) **同态基本定理**：设 $G\overset{f}{\sim}G'$(满同态),$K=\ker f$,则

① 存在同构 σ: $G/K\overset{\sigma}{\cong}G'$.

② 设 $\varphi: a\mapsto aK\ (G\to G/K)$是 G 到其商群的**自然同态**,则有 $f=\sigma\varphi$.

(2) **子群对应定理**：设 $G\overset{f}{\sim}G'$,$K=\ker f$,$S=\{H \mid K\leqslant H\leqslant G\}$,$T=\{N \mid N\leqslant G'\}$,则存在双射 $\tau: H\mapsto f(H)\ (S\to T)$.(对正规子群也有相应的对应定理.)

(注意集合 S 并非是 G 中的全部子群,只是那些包含 K 的子群.)

(3) **商群同构定理**：设 $G\overset{f}{\sim}G'$,$K=\ker f$,$K\leqslant H\lhd G$,则 $f(H)\lhd G'$,且

$$G/H\cong G'/f(H)\cong\frac{G/K}{H/K}.$$

(4) **子群乘积同构定理**：$N\lhd G$,$H\leqslant G$,则
$HN/N\cong H/(H\cap N)$. (对加群应表达为$(H+N)/N\cong H/(H\cap N)$.)

4. 自同态半群和自同构群

- **群的自同态半群**：$\mathrm{End}G=\{f \mid f: G\to G\ \text{同态}\}$.
- **群的自同构群**：$\mathrm{Aut}G=\{f \mid f: G\to G\ \text{同构}\}$.
- **群的内自同构群**：$\mathrm{Inn}G=\{\sigma_a \mid a\in G,\sigma_a(x)=axa^{-1},\forall x\in G\}$.
  (1) $\mathrm{Inn}G\lhd\mathrm{Aut}G$,$G/C(G)\cong\mathrm{Inn}G$.
  (2) $\mathrm{Aut}S_n\cong S_n\ (n\geqslant 3)$.

5. 极大正规子群与单群的关系

N 是 G 的极大正规子群$\Leftrightarrow G/N$ 是单群.

二、习题 2.8 详细解答

2.8-1 设 $f:G\to G_1$ 是同态，$\varphi:G_1\to G_2$ 是同态，则 $\varphi f:G\to G_2$ 是同态.

分析 该题完全是按定义走过场，但对初学者来说，为了熟悉概念，还必须走一下.

证 $\forall a,b\in G$，由于 $\varphi f(ab)=\varphi(f(a)f(b))=\varphi f(a)\varphi f(b)\in G_2$，所以 φf 是 G 到 G_2 的同态.

2.8-2 设 $G=\{(a,b)\mid a,b\in\mathbb{R},a\neq 0\}$ 是对乘法：$(a,b)(c,d)=(ac,ad+b)$ 所构成的群. $K=\{(1,b)\mid b\in\mathbb{R}\}$，证明

$$G/K\cong(\mathbb{R}^*,\cdot),$$

其中 $\mathbb{R}^*$ 是非零实数的乘法群.

分析 遇到证明两个群同构的问题，通常有两个方法，一是写出这两个群的元素，找出对应关系，然后证明保持运算. 这种方法与同态没有关系. 第二个方法是利用同态基本定理. 如果式子中含有商群，一般做法可描述如下：要证 $G/H\cong G'$，先找出一个 G 到 G' 的满同态，然后证明这个同态的核是 H，则由同态基本定理得到等式. 本节的大多数习题都要求用同态的方法.

证 作映射 $f:(a,b)\mapsto a(G\to\mathbb{R}^*)$，由于

$$f((a,b)(c,d))=f(ac,ad+b)=ac=f(a,b)f(c,d),$$

因而 f 是同态，且显然是满同态.

$$\begin{aligned}\ker f&=\{(a,b)\mid a\in\mathbb{R}^*,b\in\mathbb{R},f(a,b)=1\}\\&=\{(a,b)\mid a=1\}=\{(1,b)\mid b\in\mathbb{R}\}=K,\end{aligned}$$

所以由同态基本定理，得

$$G/K\cong(\mathbb{R}^*,\cdot).$$

点评 以上证明过程是最典型的，类似的题均可套用.

2.8-3 设 G 为有限 Abel 群，证明 $f:g\mapsto g^k$ 是 G 的自同构的充分必要条件是 $(k,|G|)=1$.

分析 利用自同构条件：$\ker f=1$. 还需要用到有限 Abel 群的一个性质.

证 首先应证明 $f:g\mapsto g^k$ 是 G 的一个自同态：

$$f(g_1g_2)=(g_1g_2)^k=g_1^kg_2^k=f(g_1)f(g_2).$$

先证必要性. ⇒：设 $f:g\mapsto g^k$ 是 G 的自同构，则 $\ker f=1$. 要证 $(k,|G|)=1$.

用反证法. 假设 $(k,|G|)=m\geqslant 2$. 则有素数 $p\mid m$，因而 $p\mid k$ 和 $p\mid |G|$. 由前面已知的结论：G 中有 p 阶元（主教材定理 2.6.3），设 $a\in G,o(a)=p$，则 $f(a)=a^k=e$，得 $a\in\ker f$，即 $\ker f\neq 1$，与 f 是 G 的自同构矛盾.

再证充分性. $\Leftarrow$:设$(k,|G|)=1$,要证 $f:g\mapsto g^k$ 是G的自同构. 分析 f 的核:

因为 $\ker f=\{a\in G\mid a^k=e\}$,我们来分析核中的元素,任取 $a\in\ker f$,满足 $a^k=e$,因而 $o(a)\mid k$. 另一方面,$o(a)\mid |G|$. 而$(k,|G|)=1$,故 $o(a)=1$,即 $a=e$. 所以 $\ker f=\{e\}$,因而 f 是单同态,由于有限集上的单射必是满射,所以 f 是G的自同构.

点评　这个题的关键之处是利用有限 Abel 群的性质,一般不容易想到.

2.8-4　设$G=(\mathbb{Z},+)$,$G'=\langle a\rangle$为 6 阶循环群,$\varphi:n\mapsto a^n$,$(G\to G')$,$\forall n\in\mathbb{Z}$,则 φ 是G到G'的满同态.(1)找出像为$\langle a^2\rangle$的G的所有子群.(2)找出像为$\langle a^3\rangle$的G的所有子群.

分析　首先可把 6 阶循环群写成$(\mathbb{Z}_6,+)$,则$\langle a^2\rangle=\langle\bar{2}\rangle$,$\langle a^3\rangle=\langle\bar{3}\rangle$. 然后求出它们的全原像,再找出所要求的子群. 而全原像的求法,可利用公式 $f(a)=a'\Rightarrow f^{-1}(a')=a\ker f$(如果是加群,则应为 $f^{-1}(a')=a+\ker f$),并可推广到子群:$f(H)=H'\Rightarrow f^{-1}(H')=\bigcup_{a'\in H'}a\ker f$.

解　可设$G'=(\mathbb{Z}_6,+)$,则 $\varphi:n\mapsto\bar{n}$,由于

$$\varphi(n_1+n_2)=\overline{n_1+n_2}=\overline{n_1}+\overline{n_2}=\varphi(n_1)+\varphi(n_2),$$

所以 φ 是G到G'的同态. $\ker\varphi=\{a\in\mathbb{Z}\mid\varphi(a)=\bar{0}\}=\{6n\mid n\in\mathbb{Z}\}$.

(1) 找出像为$\langle\bar{2}\rangle$的G的所有子群. 由于$\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4}\}$,得

$\varphi^{-1}(\bar{0})=\ker\varphi=\{6n\mid n\in\mathbb{Z}\}$,$\varphi^{-1}(\bar{2})=2+\ker\varphi=\{6n+2\mid n\in\mathbb{Z}\}$,
$\varphi^{-1}(\bar{4})=4+\ker\varphi=\{6n+4\mid n\in\mathbb{Z}\}$,

由于$\langle\bar{2}\rangle=\langle\bar{4}\rangle$,所以 $\varphi^{-1}(\bar{2})$和 $\varphi^{-1}(\bar{4})$中的元素生成的子群的像都是$\langle\bar{2}\rangle$. 因此像为$\langle\bar{2}\rangle$的G的所有子群为

$$\langle 6k+2\rangle,\quad k=0,1,\cdots,$$

和

$$\langle 6m+4\rangle,\quad m=0,1,\cdots.$$

(2) 找出像为$\langle\bar{3}\rangle$的G的所有子群. 方法类似. 由于 $\varphi^{-1}(\bar{3})=\{6n+3\mid n\in\mathbb{Z}\}$. 所以像为$\langle\bar{3}\rangle$的$G$的所有子群为

$$K_m=\langle 6m+3\rangle,\quad m=0,1,\cdots.$$

点评　该题的关键是搞清映射的像、原像和全原像的关系. 实际上是要求全原像中符合要求的所有子群. 以上方法能否推广到更加一般的问题? 另外,请大家思考一个问题:我们得到的结果是G中的多个子群对应G'中的同一

个子群，这是否与同态的子群对应定理矛盾呢？（请看本节的提要.）

子群对应定理所指的 G 中的子群必须包含核：$\varphi^{-1}(\bar{0})=\ker\varphi=\{6n\mid n\in\mathbb{Z}\}$. 在像为 $\langle\bar{2}\rangle$ 的 G 的所有子群中，包含核的子群确实只有一个：$\langle 2\rangle$. 在像为 $\langle\bar{3}\rangle$ 的 G 的所有子群中，包含核的子群确实只有一个：$\langle 3\rangle$. 其他的都不包含核.

2.8-5 利用同态基本定理证明 $(\mathbb{Q},+)/(\mathbb{Z},+)\cong U=\{a\in\mathbb{C}\mid a^n=1,n\in\mathbb{Z}^+\}$，其中 U 中的运算是复数乘法.

分析 前面提到过，凡是要证明涉及商群的同构问题，一般都用同态基本定理，而且证明过程模式化：建一个同态映射，必须是满同态，求核，应用同态基本定理. 共四步.

证 U 可进一步表示为

$$U=\{e^{\frac{i2k\pi}{n}}\mid n\in\mathbb{Z}^+,k=0,1,\cdots,n-1\}.$$

作映射 $f:q\mapsto e^{i2q\pi}((\mathbb{Q},+)\to U)$，由于

$$f(q_1+q_2)=e^{i2(q_1+q_2)\pi}=e^{i2q_1\pi}e^{i2q_2\pi}=f(q_1)f(q_2),$$

所以 f 是同态，且显然是满同态. 它的核为

$$\ker f=\{q\in\mathbb{Q}\mid e^{i2q\pi}=1\}=\{q\in\mathbb{Z}\}=(\mathbb{Z},+).$$

所以由同态基本定理得

$$(\mathbb{Q},+)/\ker f=(\mathbb{Q},+)/(\mathbb{Z},+)\cong U.$$

点评 由于这类题比较简单，主要目的是熟悉同态基本定理.

2.8-6 求 $(\mathbb{Z},+)$ 上的所有自同态，并证明 $\mathrm{End}(\mathbb{Z},+)$ 与整数乘法半群同构.

分析 求所有自同态从哪里入手呢？由于自同态的像是子群，所以可从 G 的所有子群入手，找出对应的自同态. 对于循环群，可从生成元出发，将生成元映射为不同的元素就可得到不同的自同态.

半群的同态与同构的概念与群的相应概念相同，只要求保持运算.

解与证明 由于 $(\mathbb{Z},+)=\langle 1\rangle$ 是循环群，生成元 1 的不同的像将决定不同的自同态. 设 f 是 $(\mathbb{Z},+)$ 上的任意一个自同态，如果 $f(1)=a$，则 $f(x)=ax,\forall x\in\mathbb{Z}$. 当 a 取不同的元素时得到不同的自同态. 因此 $(\mathbb{Z},+)$ 上的全部自同态为

$$\mathrm{End}(\mathbb{Z},+)=\{f_n\mid f_n(x)=nx,n\in\mathbb{Z}\}.$$

下面证明 $\mathrm{End}(\mathbb{Z},+)\cong(Z,\cdot)$：作映射

$$\sigma:n\mapsto f_n((\mathbb{Z},\cdot)\to\mathrm{End}(\mathbb{Z},+)).$$

由于 $f_n(f_m(x))=nmx=f_{nm}(x)$，得到 $f_nf_m=f_{nm}$，故有

$$\sigma(nm) = f_{nm} = f_n f_m = \sigma(n)\sigma(m).$$

易证 σ 是双射，所以 $\mathrm{End}(\mathbb{Z},+)\cong(\mathbb{Z},\cdot)$.

点评 关于 σ 是双射的证明，读者可详细写一写. 该题实际上提供了确定所有自同构和两个群之间的同构的一般方法.

请读者自己求 $\mathrm{Aut}(\mathbb{Z},+)$.

2.8-7 求$(\mathbb{Z}_n,+)$上的所有自同态和自同构.

分析 利用上题所总结的方法，抓住生成元的像：自同态可把生成元映成任何元素，而自同构必须把生成元映成生成元.

解 (1)求$(Z_n,+)$上的所有自同态. 由于$(Z_n,+)=\langle\bar{1}\rangle$，设 f 是$(Z_n,+)$上的任意一个自同态，如果 $f(\bar{1})=\bar{a}$，则 $\forall x\in Z_n$ 有 $f(x)=\bar{a}x$. 当 $\bar{a}$ 取不同的元素时得到不同的自同态. 因此$(Z_n,+)$上的全部自同态为

$$\mathrm{End}(Z_n,+) = \{f_k \mid f_k(x) = \bar{k}x, k = 0,1,\cdots,n-1\}.$$

(2) 求$(Z_n,+)$上的所有自同构. 由于自同构也是自同态，即 $\mathrm{Aut}(Z_n,+)\subseteq \mathrm{End}(Z_n,+)$，故只要在自同态中找出那些双射就可以了. 可以证明

$$f_k \text{ 是双射} \Leftrightarrow (k,n) = 1.$$

证明如下：f_k 是双射$\Leftrightarrow \exists\,\bar{a}\in Z_n: f_k(\bar{a})=\bar{1}\Leftrightarrow \bar{k}\,\bar{a}=\bar{1}\Leftrightarrow ka+qn=1\Leftrightarrow (k,n)=1$. 所以$(Z_n,+)$上的所有自同构为

$$\mathrm{Aut}(Z_n,+) = \{f_k \mid f_k(x) = \bar{k}x, (k,n) = 1\}.$$

点评 注意(2)中 f_k 是双射的条件的证明方法. 是否可利用同态核来证明?

(2)的证明可利用本题分析中指出的：自同构必须把生成元映成生成元. 由于$(Z_n,+)$的全部生成元为 $\bar{k}\in Z_n$，$(k,n)=1$，所以$(Z_n,+)$上的所有自同构为 $f_k(x)=\bar{k}x$.

2.8-8 设 K_4 为 Klein 四元群，求 $\mathrm{Aut}K_4$.

分析 如前面的习题中指出的那样，可以利用生成元来做. 但也可结合本题元素很少的特点，可把所有保持单位元不动的双射写出来，看它们是否是同构. 我们用这两种方法都做一下.

解 **方法 1** Klein 四元群可表示为

$$K_4 = \langle a,b \mid o(a) = o(b) = 2, ab = ba\rangle = \{e,a,b,c = ab\}.$$

任取 $f\in \mathrm{Aut}K_4$，设 $f(a)=x$，$f(b)=y$，因为 f 是同构映射，$x\neq y$，$x,y\in\{a,b,c\}$，且 $f(c)=f(ab)=xy$. 因此 f 可表示为

$$f = \begin{pmatrix} e & a & b & c \\ e & x & y & xy \end{pmatrix},$$

x,y 共有 6 种选择，它们都是同构，并且每一个 f 可表示为 $\{a,b,c\}$ 上的一个置换，所以

$$\mathrm{Aut}K_4 \cong S_3.$$

方法 2　直接列出群元素，写出同构映射，

$$K_4 = \{e,a,b,c\}.$$

设映射 $f=\begin{pmatrix} e & a & b & c \\ e & u & v & w \end{pmatrix}$，其中 u,v,w 为 a,b,c 的一个全排列. 由于

$$f(ab) = f(c) = w = uv = f(a)f(b),$$

那么 f 是 K_4 上的自同构，且 f 是 $\{a,b,c\}$ 上的一个置换. 反之，$\{a,b,c\}$ 上的任一个置换对应 K_4 上的一个自同构，所以

$$\mathrm{Aut}K_4 \cong S_3.$$

点评　当元素比较少的时候，用方法二较好. 读者可自己求 $\mathrm{End}K_4$ 和二面体群的自同构群(答案见第 2 章补充题).

2.8-9　$G=GL_n(\mathbb{R})$，求 $\mathrm{Inn}G$.

分析　G 是实线性群，G 上的内自同构就是相似变换，问题是如何把 $\mathrm{Inn}G$ 表示得简单.

解　取 $A\in G$，作变换

$$\tau_A(X) = AXA^{-1}, \quad \forall X \in G.$$

因而有

$$\mathrm{Inn}G = \{\tau_A \mid A \in G, \tau_A(X) = AXA^{-1}\}.$$

我们可以利用有关定理，把它表示得更简单一些. 我们知道 $G=GL_n(\mathbb{R})$ 的中心为

$$C(G) = \{aI \mid a \in \mathbb{R}^*\},$$

因而由主教材定理 2.8.6 得

$$\mathrm{Inn}G = G/C(G) = \{AC(G) \mid A \in G\}.$$

每一个陪集可以表示为

$$AC(G) = A\{aI \mid a \in \mathbb{R}^*\} = \frac{A}{|A|}\{aI \mid a \in \mathbb{R}^*\}$$
$$= B\{aI \mid a \in \mathbb{R}^*\},$$
$$|B| = 1.$$

所以

$$\mathrm{Inn}G = G/C(G) \cong \{B \in G \mid |B| = 1\}.$$

即 $\mathrm{Inn}G$ 同构于行列式为 1 的实矩阵所成的群.

点评　对于初学者来说，不会想到做第二部分.

2.8-10 设 G 是单群，且不是可换群，则 $G \cong \text{Inn}G$.

分析 显然仍然利用主教材定理 2.8.6.

证 由于涉及 $\text{Inn}G$，自然会想到利用定理 2.8.6，对照一下，只需证明 $C(G)=1$ 就可以了.

考虑 G 的中心 $C(G)$，由于 $C(G) \lhd G$，G 又是单群，故 $C(G)$ 只能是 1 或 G.

由于 G 不是可换群，所以得 $C(G)=1$. 再由定理 2.8.6，得

$$\text{Inn}G \cong G/C(G) = G/1 \cong G.$$

点评 涉及概念较多，认真复习.

* **2.8-11** 设 G 有有限个子群，f 是 G 上的满自同态，证明 f 是 G 的自同构.

分析 可以想到把子群对应定理应用于同一个群上. 并利用子群个数的有限性.

证 要证 f 是 G 的自同构，只要证明 $\ker f=1$. 设

$$K = \ker f, \quad T = \{N \mid K \leqslant N \leqslant G\}, \quad S = \{H \mid H \leqslant G\}.$$

用反证法. 假设 $\ker f \neq 1$，由于 $T \subset S$，且 S 中至少比 T 多一个单位子群，所以 $|S| \geqslant |T|+1$. 另一方面，由于 f 是 G 上的满自同态，由同态的子群对应定理，存在 T 到 S 的双射，因而得到 $|S|=|T|$，矛盾. 所以

$$\ker f = 1,$$

f 是 G 的自同构.

点评 该题的条件：G 有有限个子群，是很重要的，如果没有这个条件，结论就不成立了.

2.9 群对集合的作用，Burnside 引理

一、内容提要

群对集合的作用是群的应用的桥梁，其概念有难度，对应用感兴趣的读者要多加留意.

1. 群对集合的作用的概念

我们先看一些简单作用的概念：一个函数的函数值 $f(x)$ 就称为 f 对 x 的作用. 一个置换 σ 对目标集的元素 a 的作用就是 $\sigma(a)$. 可把这个概念推广到一般的群对另外一个表面上无关系的集合的作用. 具体定义如下：

定义 A 设 G 是一个群. Ω 是一个集合(称为目标集)，G' 是 Ω 上的变换

群. 若存在一个同态 $f:G\to G'$ 满足：$\forall g_1,g_2\in G$, $\forall x\in\Omega$ 有

(1) $f(e)(x)=x$;

(2) $f(g_1g_2)(x)=f(g_1)f(g_2)(x)$.

则称 G 通过 f 作用于 Ω 上，$f(g)(x)$ 称为 g 对 x 的作用，简记为 $g(x)$.

定义 A 是通过一个同态 f 作用于另一个集合上，比较好想象. 如果这个同态 f 是同构，则称群对集合的作用 f 是忠实的. 群对集合的作用的定义的另一种形式为

定义 B 设 G 是一个群. Ω 是一个集合(称为目标集)，若对每一个 $g\in G$ 对应一个 Ω 上的变换 f_g 满足：$\forall x\in\Omega$，有

(1) $f_e(x)=x$;

(2) $f_{g_1g_2}(x)=f_{g_1}f_{g_2}(x)$.

则称 G 通过 f 作用于 Ω 上，$f_g(x)$ 称为 g 对 x 的作用，简记为 $g(x)$，这时把 g 理解为 Ω 上的变换，条件(1)(2)可简化为：(1) $e(x)=x$; (2) $g_1g_2(x)=g_1(g_2(x))$. 可证明满足条件(1)(2)的变换是可逆变换. 因此群对集合的作用就是每一个群元素对应集合上的满足条件(1)(2)的变换.

这两个定义是等价的，其本质就是 G 通过 Ω 上的一个可逆变换作用于 Ω 上. 根据具体情况决定采用哪一种形式. 为便于理解一些概念，我们可以将其想像为置换群对目标集的简单作用.

2. 作用的轨道、不动点和稳定子群

设 G 作用于 Ω 上，$a\in\Omega$.

- 以 a 为代表元的轨道：$\Omega_a=\{g(a)\mid g\in G\}$. 且有 $b\in\Omega_a\Leftrightarrow\exists g\in G$ 使 $g(a)=b\Leftrightarrow\Omega_a=\Omega_b$. 轨道是等价类.
- 不动点：$g(a)=a$，称 a 是 g 的一个不动点. 不动点是在置换的轮换表示式中可省略的元素.
- **可迁的概念**：G 在 Ω 上可迁 $\Leftrightarrow\forall a,b\in\Omega:\exists g\in G:g(a)=b\Leftrightarrow\forall a\in\Omega$ 有 $\Omega_a=\Omega$.
- **稳定子群**：$\mathrm{Stab}_G a=G_a=\{g\in G\mid g(a)=a\}$，即保持 a 不动的所有群元素的集合.
- **轨道公式**：$|\Omega_a|=[G:G_a]$, $|G|=|G_a|\cdot|\Omega_a|$.
- 同一轨道上的稳定子群是互相共轭的：$G_{g(a)}=gG_ag^{-1}$.

几种常用的作用：

- 群对自己的左平移作用：群 G，目标集 $\Omega=G$，$g(x)=gx$. 在整个目标集 Ω 上可迁. $\forall a\in\Omega$ 有 $\mathrm{Stab}_G a=1$.（右平移为：$g(x)=xg^{-1}$.）

- 群对自己的共轭作用：群 G，目标集 $\Omega=G$，$g(x)=gxg^{-1}$. 轨道是共轭类：$\Omega_a=\{gag^{-1}\mid g\in G\}$. $\mathrm{Stab}_G a=C_G(a)$.
- 群对子群集合的共轭作用：群 G，目标集 $\Omega=\{H\mid H\leqslant G\}$，$g(H)=gHg^{-1}$，轨道是共轭子群类：$\Omega_H=\{gHg^{-1}\mid g\in G\}$. $\mathrm{Stab}_G H=N_G(H)$（H 在 G 中的正规化子）.
- 群对子群左陪集集合的左乘作用：群 G，$H<G$，目标集 $\Omega=\{aH\mid a\in G\}$，$g(aH)=gaH$，可迁. $G_{aH}=aHa^{-1}$.（证明见习题 2.9-3）

3. Burnside 引理

设群 G 作用于目标集 X 上，则将 X 划分成的轨道数为

$$N=\frac{1}{|G|}\sum_{g\in G}\chi(g),$$

其中 $\chi(g)$ 为群元素 g 在 X 中的不动点的数目：$\chi(g)=|\{x\mid x\in X,g(x)=x\}|$.

群元素在目标集上的不动点的数目与群元素的类型有关. $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$-型置换在目标集上的不动点的数为 λ_1. 一般的作用也与参数 $\lambda_1,\lambda_2,\cdots,\lambda_n$ 有关.

Burnside 引理是群的应用的一个主要的公式，应该记住. 具体计算时通常列一个表进行计算.

二、习题 2.9 详细解答

2.9-1　设群 G 作用于集合 X 上，$a\in X$，Ω_a 是 a 所在的轨道，证明 $b\in\Omega_a\Leftrightarrow\Omega_a=\Omega_b$.

分析　熟悉轨道的概念，每一个轨道是一个等价类. 证明方法完全按定义来.

证　先把轨道的定义写出来.

$$\Omega_a=\{g(a)\mid g\in G\},\quad \Omega_b=\{g(b)\mid g\in G\}.$$

$\Rightarrow$：首先 $b\in\Omega_a\Rightarrow\exists\, g_1\in G$：$g_1(a)=b\Rightarrow a=g_1^{-1}(b)$. 下面证明 $\Omega_a\subseteq\Omega_b$：

$\forall g(a)\in\Omega_a$ 有 $g(a)=gg_1^{-1}(b)\in\Omega_b$，故 $\Omega_a\subseteq\Omega_b$. 类似可证 $\Omega_b\subseteq\Omega_a$. 所以 $\Omega_a=\Omega_b$.

$\Leftarrow$：显然.

综上，结论成立.

点评　该题虽然简单，作为初学者，还是应该多想一想概念.

2.9-2　设群 G 作用于 X 上，$a\in X$，$g\in G$，G_a 为 a 的稳定子群，证明 $G_{g(a)}=gG_ag^{-1}$.

分析　熟悉稳定子群的概念，还是从定义出发.

证 先写出稳定子群的定义：

$$\mathrm{Stab}_G a = G_a = \{g \in G \mid g(a) = a\}.$$

我们用互相包含的方法来证.

任取 $\sigma \in G_{g(a)}$ 有 $\sigma(g(a)) = g(a) \Rightarrow g^{-1}\sigma g(a) = a \Rightarrow g^{-1}\sigma g \in G_a \Rightarrow \sigma \in gG_a g^{-1}$，得 $G_{g(a)} \subseteq gG_a g^{-1}$.

反之，任取 $\tau \in gG_a g^{-1}$ 有 $\tau = g\varphi g^{-1}$，$\varphi \in G_a$. 于是得

$$\tau(g(a)) = g\varphi g^{-1}(g(a)) = g\varphi(a) = g(a),$$

因而 $\tau \in G_{g(a)}$ 和 $gG_a g^{-1} \subseteq G_{g(a)}$.

综上，得证.

点评 在证明过程中必须保持清醒，认清哪个是群元素，哪个是目标集元素.

2.9-3 群 $G, H \leqslant G$，目标集 $\Omega = \{aH \mid a \in G\}$，$G$ 对 Ω 的作用为：$g(aH) = gaH$. 证明满足定义的条件，并求 Ω_{aH} 与 G_{aH}.

分析 继续熟悉作用的概念.

证与解 检验：(1) $e(aH) = aH$；(2) $g_1 g_2(aH) = g_1 g_2 aH = g_1(g_2(aH))$.

求轨道 Ω_{aH}：根据定义，$\Omega_{aH} = \{gaH \mid g \in G\}$. 由于 $\forall aH, bH \in \Omega$，取 $g = ba^{-1}$，则 $g(aH) = gaH = bH$，即 aH, bH 在同一轨道上，所以 G 在 Ω 上可迁，$\Omega_{aH} = \Omega$.

求稳定子群 G_{aH}：由于 $g(aH) = aH \Leftrightarrow a^{-1}ga \in H \Leftrightarrow g \in aHa^{-1}$，所以 $G_{aH} = \{g \in G \mid g(aH) = aH\} = aHa^{-1}$.

点评 进一步熟悉作用的概念，轨道、稳定子群的概念.

2.9-4 $|G| < \infty$，$\Omega = \{K \subseteq G \mid |K| = k\}$，$G$ 对 Ω 的作用为：$g(K) = gK$. 证明满足定义的条件，问是否可迁？

分析 首先看懂题目，目标集 Ω 是 G 中的 k 元子集的集合. 这个题的难点是分析可迁性. 可从 $k = 1, 2, \cdots$ 逐个来分析，然后找出规律.

证 检验满足定义条件：(1) $e(K) = eK = K$；(2) $g_1 g_2(K) = g_1 g_2 K = g_1(g_2(K))$. 下面证可迁性：

设 $|G| = n$，下面分几种情况讨论.

当 $k = 1$ 时，就是群对本身的左平移作用，是可迁的.

当 $2 \leqslant k \leqslant n-2$ 时，则 $|\Omega| = \binom{n}{k} > n$（可用初等方法证明）. 下面用反证法证明 G 在 Ω 上不可迁：假设 G 在 Ω 上可迁，则有轨道公式：$|G| = |G_a| \cdot |\Omega_a| = |G_a| \cdot |\Omega| \geqslant |\Omega| > n$，矛盾. 所以 G 在 Ω 上不可迁.

当 $k=n-1$ 时,我们来证明 G 在 Ω 上可迁: 记 $K_x=G-x$,则 $\Omega=\{K_x \mid x\in G\}$. 任取 $a\neq b,K_a,K_b\in\Omega$,则易证 $b\notin ba^{-1}K_a$(否则,$\exists c\in K_a$ 使 $b=ba^{-1}c$,得 $c=a\in K_a$,矛盾),因而 $ba^{-1}(K_a)=ba^{-1}K_a=K_b$,所以 G 在 Ω 上可迁.

点评 这个题有一定难度. 特别是在证明当 $k=n-1$ 时,证明 G 在 Ω 上可迁时,元素 ba^{-1} 是经过试验得到的.

不妨先分析一个具体的例子,再找出一般规律.

在证明过程中我们得到一个副产品: 如果有限群 G 在 Ω 上可迁,则 $|G|\geqslant|\Omega|$;反之,如果 $|G|<|\Omega|$,则一定是不可迁的.

2.9-5 群 G 对有限集 Ω 的作用为 $g(x),g\in G,x\in\Omega$. 证明:

(1) $g(x)$ 是 Ω 上的一个置换;

(2) 令 S_Ω 是 Ω 上的对称群,则 $\varphi:g\mapsto g(x)(G\to S_\Omega)$ 是 G 到 S_Ω 的同态. 当 φ 是单同态时,称 G 对 Ω 的作用是**忠实的**.

分析 本题实际上是要证明两件事: 一是群元素在有限集 Ω 上的作用就是一个置换;二是 G 与 Ω 上的一个置换群同态或同构,当同构时,称这个作用是忠实的.

证 (1)由于有限集上的单射必为置换,故只需证明 $g(x_1)=g(x_2)\Rightarrow x_1=x_2$. 根据作用的定义有

$$g(x_1)=g(x_2)\Rightarrow g^{-1}(g(x_1))=g^{-1}(g(x_2))\Rightarrow g^{-1}g(x_1)=g^{-1}g(x_2)\Rightarrow x_1=x_2.$$

所以 g 是单射,有限集上的单射必为置换.

(2) 由于 $g(x)$ 是 Ω 上的一个置换,可记作 σ_g. 则 φ 可表示为

$$\varphi:g\mapsto\sigma_g(G\to S_\Omega),$$

由于 $\varphi(g_1g_2)=\sigma_{g_1g_2}$,而 $\sigma_{g_1g_2}(x)=g_1g_2(x)=\sigma_{g_1}(\sigma_{g_2}(x))$,故有

$$\varphi(g_1g_2)=\sigma_{g_1g_2}=\sigma_{g_1}\sigma_{g_2}=\varphi(g_1)\varphi(g_2),$$

所以 φ 是 G 到 S_Ω 的同态.

点评 通过该题了解群 G 对有限集 Ω 的作用的两种定义的等价性.

2.10 应用举例

一、内容提要

本节重点介绍群论在对称形体着色问题上的应用,并为数字通信方面所需的基础性知识作一个简要介绍.

1. 着色问题

对称形体(包括正多边形、正多面体、具有对称性的图形或结构等)的顶点或面的着色问题:

设 $X=\{1,2,\cdots,m\}$是对称形体的顶点(或面)集合,G 是对称形体的旋转群,$G\leqslant S_m$. $A=\{a_1,a_2,\cdots,a_n\}$是 n 种颜色的集合. $f:X\to A$ 是顶点的一个着色,令

$$\Omega=\{f\mid f:X\to A\}$$

是全部着色的集合,则$|\Omega|=m^n$. 定义群 G 对 Ω 的作用为

$$g(f)=fg^{-1}.$$

则本质上不同的着色方法数就是 Ω 在 G 作用下的轨道数,可用 Burnside 定理求得.

方法可应用于分子结构的同分异构体的数目、开关线路的数目和不同构的图的数目等问题的计算.

2. 二次同余方程的求解问题

由于此问题主要涉及乘法运算,所以我们在乘法群$(Z_p^*,\cdot)$中考虑问题.

设 p 是奇素数,$a\in Z_p^*$,设二次同余方程为

$$x^2\equiv a(\bmod p).$$

(1) **有解条件**:$x^2\equiv a(\bmod p)$有解$\Leftrightarrow a^{\frac{p-1}{2}}\equiv 1(\bmod p)$.

(2) **有解方程的个数**:方程只对常数项 a 取 Z_p^* 中的$\dfrac{p-1}{2}$个值有解. 换句话说,Z_p^* 中平方剩余为 a 元素的个数是$\dfrac{p-1}{2}$.

(3) **解的个数成对出现**:若 b 是解,则$-b$ 也是解,且 $b\neq -b\bmod p$.

(4) **解的表达式**:当方程 $x^2\equiv a(\bmod p)$有解时,它的解可表示为

$$x_{1,2}=\pm\sqrt{a+np}\bmod p,\quad \text{其中选 } n \text{ 使 } a+np \text{ 为平方数}.$$

当 $p\equiv 3(\bmod 4)$时,则方程 $x^2\equiv a(\bmod p)$有解时,它的解可表示为

$$x_{1,2}=\pm a^{\frac{p+1}{4}}\bmod p.$$

例如,方程 $x^2\equiv 5(\bmod 19)$的解,用两种方法均得 $x_{1,2}=\pm 9\bmod 19=9,10$.

二、习题 2.10 详细解答

2.10-1　用 3 种颜色的珠子做成 5 颗珠子的项链,可做成多少种?

分析　作为初学者必须从头开始,从建立数学模型出发,什么是目标集,

什么是群,如何作用于目标集上.

解 设 $X=\{1,2,3,4,5\}$为正5边形的顶点集合,D_5是正5边形的旋转群. $A=\{a_1,a_2,a_3\}$是颜色集合. 目标集为有标号的着色方法的集合:$\Omega=\{f\mid f:X\to A\}$. 定义 D_5对 Ω 的作用为

$$\forall g\in D_5,\quad \forall f\in\Omega \text{ 有 } g(f)=fg^{-1}.$$

则 Ω 在 D_5 的作用下的轨道数就是要求的项链数. 先写出全部群元素:

$$D_5=\{(1),(12345),(13524),(14253),(15432),(25)(34),(12)(35),$$
$$(13)(45),(14)(23),(24)(15)\}$$

其中 1^5-型置换1个,5^1-型置换4个,$1^1 2^2$-型置换5个,按类型计算群元素的不动点数目列表如下:

元素 g 的类型	$\chi(g)$	同类 g 的个数	$\sum\chi(g)$
1^5	3^5	1	3^5
5^1	3	4	12
$1^1 2^2$	3^3	5	5×3^3
		10	

由 Burnside 引理,得

$$N=\frac{3^5+4\times3+5\times3^3}{10}=\frac{3(81+4+45)}{10}=39.$$

所以共有39种项链.

点评 不可简单地套公式,应从数学模型做起.

2.10-2 在苯环上结合3个H和3个CH_3,可形成多少种化合物(将苯环上的键看作相同)?

分析 这是正六边形的顶点着色问题,但不是任意着色,而是有限制的着色. 方法要点:搞清置换群和目标集;作表计算不动点数.

解 置换群为 D_6,其中有 1^6-型置换1个,3^2-型置换2个,6^1-型置换2个,2^3-型置换4个,$1^2 2^2$-型置换4个.

设顶点集为 $X=\{1,2,3,4,5,6\}$,颜色集合为 $A=\{a_1,a_2\}$,则目标集为

$$\Omega=\{f\mid f:X\to A \text{ 且 } |f^{-1}(a_1)|=3\}.$$

不难求出 $|\Omega|=\binom{6}{3}=20$.

计算不动点数的关键是在同一个轮换里的点必须是同一种颜色. 列表计算如下:

g(G中元素)的类型	$\chi(g)$-g 在 Ω 中的不动点数	同类 g 的个数	$\sum\chi(g)$
1^6	20	1	20
$1^2 2^2$	4	3	12
2^3	0	4	0
3^2	2	2	4
6^1	0	2	0
$\sum$		12	36

由 Burnside 引理,得 $N=36/12=3$.

所以共可形成 3 种化合物.

点评 注意该题与第 1 题的不同之处,为了确切掌握概念与方法,我们还是要求从头开始,从建立数学模型开始.

2.10-3 对正六面体的面用 n 种颜色着色,问有多少种本质上不同的着色方法?

分析 我们首先可把面着色问题转化为顶点着色问题. 以每个面的中心为顶点作出一个正八面体,于是正六面体的面着色问题就转化为正八面体的顶点着色问题.

解 以每个面的中心为顶点作出一个正八面体,于是正六面体的面着色问题就转化为正八面体的顶点着色问题. 设 $X=\{1,2,3,4,5,6\}$为正 8 面体的顶点集合,由主教材例 2.4.2 可知,正六面体的旋转群 G 有 24 个元素(由习题 2.4-7,$G\cong S_4$),因而正八面体的旋转群 G 有 24 个元素. $A=\{a_1,a_2,\cdots,a_n\}$是颜色集合. 目标集为 $\Omega=\{f\mid f:X\to A\}$,$|\Omega|=n^6$. 下面我们先看 G 中的元素类型:1^6-型 1 个,$1^2 4^1$-型 6 个,$1^2 2^2$-型 3 个,3^2-型 8 个,2^3-型 6 个. 它们的不动点数列表计算如下:

g(G中元素)的类型	$\chi(g)$-g 在 Ω 中的不动点数	同类 g 的个数	$\sum\chi(g)$
1^6	n^6	1	n^6
$1^2 4^1$	n^3	6	$6n^3$
2^3	n^3	6	$6n^3$
3^2	n^2	8	$8n^2$
$1^2 2^2$	n^4	3	$3n^4$
$\sum$		24	$n^6+3n^4+12\,n^3+8n^2$

所以本质上不同的着色方法数为

$$N = \frac{n^6 + 3n^4 + 12n^3 + 8n^2}{24}.$$

点评 正六面体与正八面体是互相可以转换的，它们的旋转群相同. 类似地，正 12 面体正 20 面体是互相可以转换的，它们的旋转群相同.

2.10-4 求 5 个点的不同构的图有多少个？

分析 首先应复习前面的图的基本概念，然后把求不同构的图的问题与群的作用联系起来. 设图的点数是 n，完全图的边数是 $m=\binom{n}{2}$，设完全图的边集合为 $X=\{e_1,e_2,\cdots,e_m\}$，$A=\{0,1\}$，每一个映射 $f:X\to A$ 代表一个有标号图，其中若 $f(e)=0$，代表该边不存在；若 $f(e)=1$，代表该边存在. 故有标号图就是集合 X 的着色（两种颜色）问题. 全体带标号的图的集合就是我们要研究的目标集：$\Omega=\{f\mid f:X\to A\}$，$|\Omega|=2^{\binom{n}{2}}$. 群为点集上的对称群 $G=S_n$. 于是不同构的图的个数就是 Ω 在 G 作用下的轨道数.

解 根据已知条件，$n=5$，$m=10$，$X=\{e_1,e_2,\cdots,e_{10}\}$，$A=\{0,1\}$，$\Omega=\{f\mid f:X\to A\}$，$|\Omega|=2^{10}$. $G=S_5$. 现在来看如何计算每一个群元素在 Ω 中的不动点数. 例如，元素 $g=(1)(234)(5)\in S_5$，某个 f 是 g 的不动点：$g(f)=f$，则边(12)，(13)，(14)必须着相同的颜色，边(25)，(35)，(45)必须着相同的颜色，边(23)，(34)，(42)必须着相同的颜色，因而共有 2^3 种选择，所以 $\chi(g)=2^3=8$.（可以画一个图分析）. 按这样的方法列表计算如下：

g(G 中元素)的类型	$\chi(g)$-g 在 Ω 中的不动点数	同类 g 的个数	$\sum\chi(g)$
1^5	2^{10}	1	2^{10}
$1^3 2^1$	2^7	10	10×2^7
$1^2 3^1$	2^4	20	$20\times n^3$
$1^1 4^1$	2^3	30	30×2^3
$1^1 2^2$	2^6	15	15×2^6
$2^1 3^1$	2^3	20	20×2^3
5^1	2^2	24	24×2^2
$\sum$		120	4080

所以 5 个点的不同构的图的个数为

$$N = 4080/120 = 34.$$

点评 对于所得的结果可用画图的方法检验是否正确. 可按边数分类：边数为0,只有1个;边数为1,也只有1个;边数为2,有2个;……. 虽然有点麻烦,但并不难.

2.11 群的直积与有限可换群

一、内容提要

如何把一个复杂的群用简单的群表示出来,群的直积就是一种方法. 对有限可换群,用直积的方法可把所有的群都表达出来,所以这节的内容对有限可换群是终结性的.

群的直积

- 定义 设$(G_1,\cdot)$,$(G_2,\circ)$是两个群,$G_1\times G_2=\{(a,b)\mid a\in G_1,b\in G_2\}$($G_1$与$G_2$的笛卡儿积),在$G_1\times G_2$中定义乘法：$(a_1,b_1)(a_2,b_2)=(a_1\cdot a_2,b_1\circ b_2)$,则$G_1\times G_2$对此乘法构成群,称为$G_1$与$G_2$的直积.
  群的直积的用途主要是把一个复杂的群表示为简单的群的直积.
- 群可表示为子群的直积的条件：设$A,B\leqslant G$,满足：(1)$A,B\lhd G$,(2)$G=AB$,(3)$A\cap B=1$. 则$G=A\times B$.
- 有限可换群可表示为循环群的直积,有两种表示方法：设G可换,且$|G|=n$.

(1) 有限可换群的初等因子表示式：设$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$($p_1,p_2,\cdots,p_s$为素数,但不要求不同,称$p_1^{\alpha_1},p_2^{\alpha_2},\cdots,p_s^{\alpha_s}$为$n$的一个初等因子组). G可表示为：$G=C_{p_1^{\alpha_1}}\times C_{p_2^{\alpha_2}}\times\cdots\times C_{p_s^{\alpha_s}}$. 由于一个整数有不同的初等因子组,因而$G$可能有互不同构的群,每一个初等因子组对应一个结构.

(2) 有限可换群的不变因子表示式：G可表示为：$G=C_{h_1}\times C_{h_2}\times\cdots\times C_{h_t}$,其中$n=h_1h_2\cdots h_t$且$h_2\mid h_1,h_3\mid h_2,\cdots,h_t\mid h_{t-1}$($h_1,h_2,\cdots,h_t$称为$n$的一个不变因子组). 可将每个初等因子组变为不变因子组. 因而同一个有限可换群可有两种表示方法. 比较来说,有限可换群的不变因子表示法要简单一些.

- 整数的初等因子组和不变因子组的计算方法：设$n=p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$,$p_1$,$p_2,\cdots,p_t$为互不相同的素数,则
  (1) 把每一个指数作一个分拆,就得到一个初等因子组.
  (2) 由每一个初等因子组逐次取不同底的最高次幂,可得一个不变因子组.
- 由有限可换群的初等因子和不变因子表示式可以得到以下结果：

(1) n 阶有限可换群的个数可求出.(见习题 2.11-7)

(2) 有限可换群中任何一个元素的阶可整除群中元素的最高阶.这个结果以后有用.

二、习题 2.11 详细解答

2.11-1 设 G 是群,G_1,G_2 是 G 的正规子群,且 $G=\langle G_1,G_2\rangle$,$G_1\cap G_2=\{e\}$,证明

$$G\cong G_1\times G_2.$$

分析 此题与主教材定理 2.11.2 比较,只差一点点:条件(2).

证 由定理 2.11.2,只需证明 $G=G_1G_2$.

显然有 $G_1G_2\subseteq G$.

反之,任取 $g\in G$,因 $g\in\langle G_1,G_2\rangle$和 G_1,G_2 是 G 的正规子群,g 可表示为

$$g=ab,\quad a\in G_1,\quad b\in G_2,$$

所以 $g\in G_1G_2$,因而 $G\subseteq G_1G_2$

综上得 $G=G_1G_2$.

由本节定理 2.11.2,得 $G=G_1G_2\cong G_1\times G_2$.

分析 该题的主要目的是熟悉定理 2.11.2.虽然证明很简单.

2.11-2 证明$\mathbb{Z}/\langle 6\rangle\cong\mathbb{Z}/\langle 2\rangle\times\mathbb{Z}/\langle 3\rangle$.

分析 首先要理解符号的意义,然后利用定理 2.11.2.

证 首先要理解符号的意义.实际上就是证明以下命题:

$$(\mathbb{Z}_6,+)\cong(\mathbb{Z}_2,+)\times(\mathbb{Z}_3,+).$$

再利用我们前面给出的符号,可以表示得简单一些:

$$C_6\cong C_2\times C_3.$$

如果直接用循环群的不变因子表示法,这个题目就不用做了.我们现在要利用本节定理 2.11.2 来做本题.定理 2.11.2 有三个条件:

(1) 由于循环群是可换群,它的子群都是正规子群,即 $C_2\lhd C_6$,$C_3\lhd C_6$.

(2) $C_2+C_3=\{k\bar{2}+l\bar{3}\mid k,l\in\mathbb{Z}\}=C_6$.

(3) $C_2\cap C_3=\{\bar{0}\}$.

所以 $C_6\cong C_2\times C_3$.

点评 注意$(\mathbb{Z}_2,+)\times(\mathbb{Z}_3,+)$是笛卡儿积.令$\mathbb{Z}_2=\{\bar{0},\bar{1}\}$,$\mathbb{Z}_3=\{\tilde{0},\tilde{1},\tilde{2}\}$,则

$$\begin{aligned}(\mathbb{Z}_2,+)\times(\mathbb{Z}_3,+)&=\{(\bar{0},\tilde{0}),(\bar{0},\tilde{1}),(\bar{0},\tilde{2}),(\bar{1},\tilde{0}),(\bar{1},\tilde{1}),(\bar{1},\tilde{2})\}\\&=\langle(\bar{1},\tilde{1})\rangle\cong(\mathbb{Z}_6,+).\end{aligned}$$

其中 $\bar{k}$ 表示模 2 的同余类，$\widetilde{m}$ 表示模 3 的同余类.

2.11-3 设 $G=G_1\times G_2$，证明 $G/G_1\cong G_2$，$G/G_2\cong G_1$.

分析 进一步熟悉群的直积的概念，首先看清题目，G_1，G_2 并不是 G 的子群，怎么能做商群呢？这就要利用同构的关系.

证 令 $H_1=G_1\times\{e_2\}$，其中 e_2 是 G_2 的单位元，则 $H_1\leqslant G_1\times G_2$，且 $H_1\cong G_1$；令 $H_2=\{e_1\}\times G_2$，其中 e_1 是 G_1 的单位元，则 $H_2\leqslant G_1\times G_2$，且 $H_2\cong G_2$.

进一步还要证明 H_1，H_2 是 $G=G_1\times G_2$ 的正规子群：$\forall g=(x,y)\in G$，$h=(a,e_2)\in H_1$，有

$$ghg^{-1}=(xax^{-1},e_2)\in H_1,\quad 故\ H_1\lhd G;\quad 类似可证\ H_2\lhd G.$$

这样，题目给出的商群就有意义了：

$$G/G_1\cong G/H_1,\quad G/G_2\cong G/H_2.$$

下面证明同构，通常的方法是利用同态基本定理（当然用陪集表示式也可以）.

作映射 $f:(a,b)\mapsto b(G\to G_2)$. 由于

$$\begin{aligned}f((a_1,b_1)(a_2,b_2))&=f((a_1a_2,b_1b_2))=b_1b_2\\&=f((a_1,b_1))f((a_2,b_2)),\end{aligned}$$

所以 f 是同态，且显然是满的. 下面求它的核：

$$\begin{aligned}\ker f&=\{(a,b)\in G\mid f(a,b)=b=e_2\}=\{(a,e_2)\mid a\in G_1\}\\&=G_1\times\{e_2\}=H_1\cong G_1.\end{aligned}$$

所以由同态基本定理，得

$$G/G_1\cong G_2.$$

类似可证 $G/G_2\cong G_1$.

点评 做该题概念要十分清楚.

2.11-4 设 $A,B\leqslant G$，$G\cong A\times B$，$N\unlhd A$，证明

$$G/N\cong(A/N)\times B.$$

分析 首先看一下题的意义，N 是 A 的正规子群，但不能马上得出 N 也是 G 的正规子群，因此左边的商群还需要证明是存在的. 为此，我们可先把右边的元素写出来，然后利用同态基本定理来证.

证 先把右边的元素写出来，$A/N=\{aN\mid a\in A\}$，因而

$$(A/N)\times B=\{(aN,b)\mid a\in A,b\in B\}.$$

再把 G 的元素用直积写出：

$$G\cong A\times B=\{(a,b)\mid a\in A,b\in B\}.$$

这样,同态映射就很容易找出了.作映射:

$$f:(a,b)\mapsto(aN,b)\quad(G\to(A/N)\times B).$$

由于

$$\begin{aligned}f((a_1,b_1)(a_2,b_2))&=f((a_1a_2,b_1b_2))=(a_1a_2N,b_1b_2)\\&=(a_1N,b_1)(a_2N,b_2)\\&=f((a_1,b_1))f((a_2,b_2)).\end{aligned}$$

所以 f 是同态,且显然是满同态.

求核:

$$\begin{aligned}\ker f&=\{(a,b)\mid f(a,b)=(N,e)\}\\&=\{(a,b)\mid(aN,b)=(N,e)\}\\&=(N,e)\cong N.\end{aligned}$$

所以由同态基本定理得

$$G/N\cong(A/N)\times B.$$

点评 该题涉及的概念比较多,必须仔细做.

2.11-5 写出 45 阶可换群的一切可能类型.

分析 我们不妨用两种方法做,然后比较结果有什么不同.

解 由于 $45=5\times3^2$,45 的初等因子组有

$$\{5,3^2\},\quad\{5,3,3\}.$$

因而群可表示为

$$C_5\times C_9,\quad C_5\times C_3\times C_3.$$

由初等因子组可求出不变因子组,具体求法为:逐次取不同底数的最高次幂.有

$$\{45\},\quad\{15,3\}.$$

所以 45 阶可换群的一切可能的类型有

$$C_{45},\quad C_{15}\times C_3.$$

点评 比较这两种表示方法,可见用不变因子组方法所得结果简单一些.

2.11-6 写出 144 阶可换群的一切可能类型.

分析 由于用不变因子组方法所得结果简单一些,所以我们以后采用不变因子组方法.但是为了求得整数的不变因子组,还是先求初等因子组,再把每一个初等因子组变为不变因子组.

解 由于 $144=2^4\times3^2$,144 的初等因子组有

$\{2^4,3^2\}$, $\{2^3,2,3^2\}$, $\{2^2,2^2,3^2\}$, $\{2^2,2,2,3^2\}$, $\{2,2,2,2,3^2\}$,

$\{2^4,3,3\}$, $\{2^3,2,3,3\}$, $\{2^2,2^2,3,3\}$, $\{2^2,2,2,3,3\}$,

$$\{2,2,2,2,3,3\}.$$

由每一个初等因子组用前面指出的逐次取不同底数的最高次幂的方法，求出不变因子组，得到不变因子组：

$$\{144\},\quad \{72,2\},\quad \{36,4\},\quad \{36,2,2\},\quad \{18,2,2,2\},$$
$$\{48,3\},\quad \{27,6\},\quad \{12,12\},\quad \{12,6,2\},\quad \{6,6,2,2\}.$$

所以 144 阶可换群的一切可能的类型有

$$C_{144},C_{72}\times C_2,C_{36}\times C_4,C_{36}\times C_2\times C_2,C_{18}\times C_2\times C_2\times C_2,$$
$$C_{48}\times C_3,C_{27}\times C_6,C_{12}\times C_{12},C_{12}\times C_6\times C_2,C_6\times C_6\times C_2\times C_2.$$

点评 做完这个题，可以说对初等因子组和不变因子组的概念和计算方法有了比较好的了解.

2.11-7 试求 n 阶交换群的可能类型数.

分析 由于在写出初等因子组时，涉及整数的分拆，而整数的分拆是组合数学研究的问题. 读者可能没有学过组合数学，不要紧，概念本身很简单：例如，4 可分拆为：4，3+1，2+2，2+1+1，1+1+1+1，总共有 5 种分拆. 有关分拆的内容可参考离散数学手册[3]和组合数学[4].

解 设 n 的标准分解式为

$$n = p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}.$$

设 $P(m)$ 为整数 m 的分拆数，例如 $P(4)=5$，一般的计算方法见组合数学的书.

由此得 n 阶交换群的可能的类型数为

$$\prod_{i=1}^{s}P(n_i).$$

点评 由于整数的分拆数还没有一个紧凑的公式，所以我们只能得到以上的表达式. 我们不妨把习题 2.11-6 作为例子来看一下. 设 $144=2^4\times 3^2$，4 有 5 种分拆：4，3+1，2+2，2+1+1，1+1+1+1，2 有 2 种分拆：2，1+1，所以共有 10 种互不同构的 144 阶可换群.

2.12 有限群的结构，Sylow 定理

一、内容提要

有限可换群的结构已完全解决. 对有限非可换群的结构主要根据西罗定理来分析，这是群论中比较难的部分，其结果也没有有限可换群那么完美.

1. 子群与 Sylow p-子群的概念

- **p-子群**：设 $|G|<\infty$，$H\leqslant G$ 且 $|H|=p^k$（p 为素数），则称 H 是 G 的

p-子群.

- **Sylow$p$-子群**：设 H 是 G 的 p-子群，$|H|=p^{\alpha}$ 且 $p^{\alpha+1}\nmid|G|$，则称 H 是 G 的 Sylow p-子群. 即 H 是 G 中 p 的最高次幂的 p-子群.

2. Sylow 定理

设 $|G|=p^{\alpha}n_1$，$(p,n_1)=1$，则

(1) **存在定理**：G 中存在 $p^k(1\leqslant k\leqslant\alpha)$ 阶子群.

(2) **包含定理**：任何一个 p^k 阶子群被包含在一个 Sylow p-子群之中.

(3) **共轭定理**：任何两个 Sylow p-子群互相共轭.

(4) **计数定理**：G 中 Sylow p-子群的个数 $N(p^{\alpha})$ 满足：$N(p^{\alpha})\equiv1 \pmod p$ 和 $N(p^{\alpha})=[G:N_G(P)]$. 其中 P 为任一 Sylow p-子群，$N_G(P)$ 为 P 在 G 中的正规化子.

注意本书引入记号 $N(p^{\alpha})$ 表示 Sylow p-子群的个数. 不要与记号 $N_G(P)$ 搞混.

3. 若干结果

(1) 对任何有限群 G，若 $p\,||G|$，则 G 中有 p 阶元和 p-子群.(此结果在本习题集中前面已提前证明了.)

(2) 设 $H\lhd G$，若 H 包含 G 的一个 Sylow p-子群，则 H 包含 G 的所有 Sylow p-子群.

(3) G 中 Sylow p-子群的个数 $N(p^{\alpha})$ 满足：$N(p^{\alpha})\,||G|$.

(4) 如果 G 中存在惟一的 m 阶子群，则此子群必为正规子群.

(5) 12 阶非可换群只有 A_4，D_6 或 $T=\langle a,b\,|\,o(a)=6,o(b)=4,ba=a^{-1}b,b^2=a^3\rangle$.($T=\{a^i,a^ib\,|\,i=0,1,\cdots,5\}$，乘法表：$o(a)=6,o(b)=4,ba=a^{-1}b,b^2=a^3$.)

思考题：证明有限可换群的结构定理.

二、习题 2.12 详细解答

2.12-1 证明 145 阶群是循环群.

分析 首先写出阶数的标准分解式：$145=5\times29$，是两个素数的乘积，我们以前遇到过，问题看起来比较简单. 只要能证明 $G=C_5\times C_{29}$，问题就解决了.

证 由于 $|G|=5\times29$，由 Sylow 定理，G 中存在 5 阶子群 C_5 和 29 阶子群 C_{29}，如果它们是正规子群，问题就解决了.

首先，G 中的 C_{29} 是惟一的 29 阶子群，所以 $C_{29}\lhd G$.

其次，再看 C_5 是否是惟一的. 可用 Sylow 定理的计数定理来分析. 设 G

中的 Sylow 5-子群的个数为 $N(5)$，则由 Sylow 定理的计数定理知 $N(5)\equiv 1(\bmod 5)$，可令$N(5)=5q+1$. 另一方面，$N(5)\,\|G|$，即 $N(5)\mid 145$，因而有 $N(5)=1$，所以$C_5\lhd G$.

显然 $C_5\cap C_{29}=1$. 综上，由群可表示为子群的直积的定理，得到

$$G=C_5\times C_{29}=C_{145},$$

所以 G 是循环群.

点评 开始的时候，我们要尽量说得详细一些，不可到处用"显然"来代替.

2.12-2 确定 S_4 中不同的 Sylow 子群的个数.

分析 由于 S_4 的阶数不大，我们不用任何理论就可把所有的 Sylow 子群找出来. 当然，这不是该题的本意. 我们要通过 Sylow 定理来确定 Sylow 子群的个数.

解 首先，写出阶数的标准分解式：$|S_4|=24=2^3\times 3$.

设 Sylow 2-子群的个数为 $N(2^3)$，Sylow 3-子群的个数为 $N(3)$. 先讨论 $N(3)$.

(1) 求 $N(3)$：由 Sylow 定理的计数定理，可设 $N(3)=3k+1$，且 $N(3)\mid 24$，得 $k=0$ 或 1. 由于 S_4 中有多个 3 阶子群，所以 $N(3)=4$.

(2) 求 $N(2^3)$：由 Sylow 定理的计数定理，可设 $N(2^3)=2k+1$，且 $N(2^3)\mid 24$，得 $k=0$ 或 1. 如果 $k=0$，即 $N(2^3)=1$，则 S_4 中有惟一的 8-子群，设为 P_8，且 $P_8\lhd S_4$. P_8 中含有四阶元、二阶元和所有同类型的元素，数目远远超过 8. 所以必有 $N(2^3)=3$.

综上，S_4 中的 Sylow 子群的个数为：$N(3)=4$ 和 $N(2^3)=3$.

点评 作为验证，我们可把所有的 Sylow 子群写出来：

三阶子群有：$\langle(123)\rangle$，$\langle(124)\rangle$，$\langle(134)\rangle$，$\langle(234)\rangle$.

八阶子群有(考虑 3 个不同的 D_4)：$\langle(1234),(24)\rangle$，$\langle(1324),(34)\rangle$，$\langle(1243),(23)\rangle$.

2.12-3 证明 40 阶群不是单群.

分析 问题等价于证明 40 阶群有非平凡正规子群. 方法仍然是首先写出阶数的标准分解式，然后考虑群内的 Sylow 子群，能否在这些 Sylow 子群中找到非平凡正规子群.

证 $|G|=40=2^3\times 5$.

考虑 Sylow 5-子群，由 Sylow 定理的计数定理，Sylow 5-子群的个数为

$$N(5)=5k+1,\quad \text{且满足 } N(5)\mid 40.$$

得 $k=0$ 和 $N(5)=1$，即有惟一的 Sylow 5-子群 P，由它的惟一性知 $P\lhd G$，且

P 是非平凡正规子群，所以 G 不是单群.

点评　该题的方法完全与书中例题类似. 更多的例子读者可在本章的补充题中找到.

2.12-4　设 p,q 是素数，证明 pq 阶群不是单群.

分析　对 pq 阶群我们比较熟悉，但我们尽量用 Sylow 定理来证明. 由于题中没有规定 p,q 是不同的素数，所以我们要分两种情况来讨论.

证　分两种情况讨论：

(1) $p=q, |G|=p^2$，我们知道 G 是可换群（习题 2.7-4），且 G 中有 p 阶元，设为 a. 则 $\langle a\rangle \lhd G$，所以 G 不是单群.

(2) $p\neq q, |G|=pq$，可设 $p>q$. 由 Sylow 定理，G 中有 p 阶子群 P. 且所有 p 阶子群的个数 $N(p)$ 满足：$N(p)=pk+1$ 和 $N(p)\mid pq$. 必有 $N(p)=1$，所以 $P\lhd G$，G 不是单群.

点评　其实，第(2)种情况早就知道 p 阶子群是正规子群（见习题 2.7-5）. 这里从 Sylow 定理再次证明这个事实.

2.12-5　p 为素数，$p\mid |G|$，$N\unlhd G$，$\left(p,\left|\dfrac{G}{N}\right|\right)=1$，则 N 包含所有的 Sylow$p$-子群.

分析　乍一看好像问题比较复杂，但细看，从直观上想像，N 已是一个阶数含有 p 的最高次幂的子群，因而也是一个包含 Sylow$p$-子群的正规子群，再利用 Sylow 定理的共轭定理，G 中的其他 Sylow$p$-子群都互相共轭，因而也在 N 中. 问题是如何将上述分析表达出来.

证　设 $|G|=p^{\alpha}n_1$，$(n_1,p)=1$. 由 $\left(p,\left|\dfrac{G}{N}\right|\right)=1$，得 $|N|=p^{\alpha}n_2$，且 $(n_2,p)=1$. 由Sylow 定理的存在定理，N 中有 p^{α} 阶子群，设为 P. 设 Q 是 G 中任意一个 p^{α} 阶子群，由 Sylow 定理的共轭定理，Q 与 P 共轭，因而存在 $g\in G$ 使 $Q=gPg^{-1}$. 因为 $P\leqslant N\lhd G$，得 $Q=gPg^{-1}\leqslant gNg^{-1}=N$. 所以 N 包含所有的 Sylow$p$-子群.

点评　这是 Sylow 定理的共轭定理的一个很好的应用.

第 2 章补充题

补充题 2-1　求没有不动点的 n 次置换的个数.

分析　我们知道每个 n 次置换的类型可表示为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$-型，没有不动点的 n 次置换就是 $\lambda_1=0$ 的置换. 我们可从相反的角度来考虑，求出含有至少一个不动点的置换的个数. 然后利用包含与排斥原理求出不含不动点的 n 次

置换的个数.

解 我们考虑含有至少一个不动点的置换的个数,例如含有1作为不动点的置换的个数,为此我们用置换的两行形式来表示这样的置换:

$$\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & i_2 & \cdots & i_n\end{pmatrix},$$

显然这样的置换的个数为$(n-1)!$. 令 A_k 为含有 k 作为不动点的置换的集合,则

$$|A_k|=(n-1)!,\quad k=1,2,\cdots,n.$$

$|A_k\cap A_l|=(n-2)!$,$|A_k\cap A_l\cap A_m|=(n-3)!$,等等. 于是,由包含与排斥原理,没有不动点的 n 次置换的个数为

$$\begin{aligned}n!-\left|\bigcup_{k=1}^{n}A_k\right|&=n!-\sum_{k=1}^{n}|A_k|+\sum_{1\leqslant k<l\leqslant n}|A_k\cap A_l|-\cdots+(-1)^n\left|\bigcap_{k=1}^{n}A_k\right|\\&=n!-\binom{n}{1}(n-1)!+\binom{n}{2}(n-2)!-\cdots+(-1)^n\binom{n}{n}\\&=n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\cdots+(-1)^n\frac{1}{n!}\right).\end{aligned}$$

点评 读者不妨用具体的例子来检验,例如 $n=4$.

补充题 2-2 设 $N\lhd A_n(n\geqslant 3)$,若 N 包含一个3-轮换,则 $N=A_n$.

分析 因为我们已知 $A_n=\langle(123),(124),\cdots,(12n)\rangle$,于是问题转化为证明 N 包含$(123),(124),\cdots,(12n)$就可以了.

证 设 N 包含一个3-轮换(α,β,γ),由于目标集中 n 个元素,谁是1谁是2…是可以重新命名的,所以我们可以认为 N 包含一个3-轮换$(1,2,3)$. 下面分两种情况来讨论:

(1) $n=3$. 设 N 包含一个3-轮换(123),则$\langle(123)\rangle\leqslant N$,所以 $N=A_3$.

(2) $n\geqslant 4$. 设 N 包含一个3-轮换(123). 由置换的共轭变换公式,取 $\tau=(12)(3i)\in A_n$,则

$$\tau\sigma\tau^{-1}=(\tau(1),\tau(2),\tau(3))=(2,1,i).$$

因为 $N\lhd A_n$,所以$(21i)\in N$,$(21i)^2=(12i)\in N$. 由于 i 可任取,因而得$(123),(124),\cdots,(12n)$属于 N,即 $N\geqslant A_n$. 所以 $N=A_n$.

点评 这个问题我们在证明 $A_n(n\geqslant 5)$是单群的定理2.7.7时已经证明了. 我们只是用更加直接的方法再证明一下.

补充题 2-3 设 $a,b\in G$,$o(a)=m$,$o(b)=n$,且 $ab=ba$,$\langle a\rangle\cap\langle b\rangle=1\Rightarrow o(ab)=?$.

分析 我们已知的结果是:$o(a)=m$,$o(b)=n$ 且 $ab=ba$,$(m,n)=1\Rightarrow$

$o(ab)=mn$. 现在不同的地方是条件$(m,n)=1$ 换成了$\langle a\rangle\cap\langle b\rangle=1$. 我们可大胆猜想其结果是 $o(ab)=\frac{mn}{d},(m,n)=d$.

解 令$(m,n)=d,r=\frac{mn}{d},s=o(ab)$.

由于$(ab)^r=(ab)^{\frac{mn}{d}}=a^{m\frac{n}{d}}b^{n\frac{m}{d}}=e$,所以 $s|r$.

另一方面,$(ab)^s=a^sb^s=e$,得 $a^s=b^{-s}$. 由条件$\langle a\rangle\cap\langle b\rangle=1$ 得 $a^s=b^{-s}=e$,因而 $m|s$ 和 $n|s$,所以$[m,n]|s$,即 $r|s$.

综上得 $r=s$,即 $o(ab)=\frac{mn}{d}$.

点评 此结果比原来的结果更一般,由$(m,n)=1$ 可推出$\langle a\rangle\cap\langle b\rangle=1$.

补充题 2-4 证明由两个二阶元生成的有限群同构于 K_4 或 $D_n(n\geqslant 3)$.

分析 我们已经熟悉 Klein 四元群 $K_4=\langle a,b\,|\,o(a)=o(b)=2,ab=ba\rangle$和二面体群 $D_n=\langle \pi_k,\pi_l\,|\,(k-l,n)=1\rangle$都是由两个二阶元生成的. 现在的问题是要证明逆命题:两个二阶元生成的有限群同构于这两个群.

证 设 G 是由两个二阶元生成的有限群:

$$G=\langle b,c\mid o(b)=o(c)=2\rangle.$$

令 $a=bc$,设 $o(a)=n$,则 $ba=c=a^{-1}b$. 所以

$$G=\langle a,b\mid o(a)=n,o(b)=2,ba=a^{-1}b\rangle\cong D_n.$$

当 $n=2$ 时,$G\cong K_4$.

点评 该题并不难,主要是熟悉生成群的概念.

补充题 2-5 求与 8 阶四元数群 $Q_8=\{\pm E,\pm I,\pm J,\pm K\}$同构的置换群.

分析 对 8 阶置换群我们熟悉的是 D_4,显然它与 Q_8 不同构. 所以我们只能用 Cayley 定理来做.

解 令 $E=1,I=2,J=3,K=4,-E=5,-I=6,-J=7,-K=8$. 下面来计算 Q_8 的每一个元素对应的置换,利用运算规则:$I^2=J^2=K^2=-E$,$IJ=K=-JI,JK=I=-KJ,KI=J=-IK$,得

$$E:(1),$$
$$I:\sigma_I=IQ_8=(1256)(3478),$$
$$J:\sigma_J=JQ_8=(1357)(2864),$$
$$K:\sigma_K=KQ_8=(1458)(2367),$$
$$-E:\sigma_{-E}=-EQ_8=(15)(26)(37)(48),$$
$$-I:\sigma_{-I}=-IQ_8=\sigma_I^{-1}=(1652)(3874),$$

$$-J: \sigma_{-J} = \sigma_J^{-1} = (1753)(2468),$$
$$-K: \sigma_{-K} = \sigma_K^{-1} = (1854)(2763).$$

所以由 Cayley 定理,得

$$Q_8 \cong \{(1),(15)(26)(37)(48),(1256)(3478),(1357)(2864),(1458)(2367),(1652)(3874),(1753)(2468),(1854)(2763)\}$$

点评 我们可以利用生成元把 Q_8 表示得简单一些. Q_8 可表示为

$$Q_8 = \langle I, J\rangle,$$

所以

$$Q_8 \cong \langle (1357)(2864),(1458)(2367)\rangle.$$

补充题 2-6 证明由两个 2 阶元生成的无限群同构于以下的线性群:

$$G = \left\{\begin{bmatrix}1 & n\\ 0 & \pm 1\end{bmatrix} \middle| n \in \mathbb{Z}\right\}.$$

分析 要证明两个群同构,首先要写出这两个群的一般元素,然后找出对应关系,并证明保持运算.

证 类似于上一题,由两个 2 阶元生成的无限群可表示为

$$D_\infty = \langle a, b \mid o(a) = \infty, o(b) = 2, ba = a^{-1}b\rangle,$$

进一步可表示为

$$D_\infty = \{a^ib^j \mid i \in \mathbb{Z}, j = 0,1\}.$$

在 G 中取 $A=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, $B=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$, 则 $o(A)=\infty$, $o(B)=2$, 且有 $BA=A^{-1}B$, 因而 G 可表示为

$$G = \{A^iB^j \mid i \in \mathbb{Z}, j = 0,1\}.$$

作映射 $f: a^ib^j \mapsto A^iB^j (D_\infty \to G)$, 显然 f 是双射, 且 $\forall x = a^ib^j, y = a^kb^l \in D_\infty$ 有

$$f(xy) = f(a^ib^ja^ka^l) = f(a^{i-k}b^{j+l})$$
$$= A^{i-k}B^{j+l} = A^iB^jA^kB^l = f(x)f(y)$$

所以

$$D_\infty \cong G.$$

点评 该题看起来复杂,实际上是"例行公务"式的证明,并无多大的技巧.

补充题 2-7 证明 $\mathrm{Aut}D_n = \left\{\begin{bmatrix}1 & 0\\ b & a\end{bmatrix} \middle| a \in Z_n^*, b \in Z_n\right\}, n \geqslant 3$.

分析 先看懂题目,左边是二面体群 D_n 的自同构群,右边是一个矩阵群,矩阵的元素是模 n 的同余类,矩阵作乘法时,涉及模 n 的加法和乘法.

首先要把左边的二面体群 D_n 的自同构群表达出来，为此，我们利用二面体群 D_n 的代数表达式：$D_n=\langle a,b\mid o(a)=n,o(b)=2,ba=a^{-1}b\rangle$，$D_n$ 的自同构必然保持元素的阶不变，由此可以求出 D_n 的自同构群.

证 我们先求 D_n 的自同构群 $\mathrm{Aut}D_n$. 设

$D_n=\langle a,b\mid o(a)=n,o(b)=2,ba=a^{-1}b\rangle=\{a^i,a^ib\mid 0\leqslant i\leqslant n-1\}$，若 $f\in\mathrm{Aut}D_n$，它保持元素的阶不变，因而有 $f(a)=a^k,(k,n)=1$；$f(b)=a^lb$，$l\in[0,n-1]$. $f(a^i)=a^{ki}$，$f(a^ib)=a^{ki+l}b$. 由于不同的 k,l 对应不同的自同构，应采用不同的记号，所以我们令

$$f_{k,l}:a^ib^j\mapsto a^{ki+l}b^j(D_n\to D_n),\quad k\in Z_n^*,\quad l\in Z_n.$$

则由以上推导知 $f_{k,l}$ 是 D_n 上的自同构(当然可以重新证明满足同构条件). 因而得

$$\mathrm{Aut}D_n=\{f_{k,l}\mid k\in Z_n^*,l\in Z_n\}.$$

下一步要证明 $\mathrm{Aut}D_n$ 与题中右边的矩阵群同构，为此，我们还需看一下 $\mathrm{Aut}D_n$ 中变换的乘法规律. 设 $f_{k,l},f_{r,s}\in\mathrm{Aut}D_n$，则

$$f_{k,l}f_{r,s}(a^ib^j)=f_{k,l}(a^{ri+s}b^j)=a^{k(ri+s)+l}b^j=a^{kri+ks+l}b^j=f_{kr,ks+l}(a^ib^j),$$

所以

$$f_{k,l}f_{r,s}=f_{kr,ks+l}.$$

作映射

$$\varphi:f_{k,l}\mapsto\begin{bmatrix}1 & l\\0 & k\end{bmatrix}(\mathrm{Aut}D_n\to G),$$

显然是双射，

$$\varphi(f_{k,l}f_{r,s})=\varphi(f_{kr,ks+l})=\begin{bmatrix}1 & 0\\ks+l & kr\end{bmatrix}=\begin{bmatrix}1 & 0\\l & k\end{bmatrix}\begin{bmatrix}1 & 0\\s & r\end{bmatrix}=\varphi(f_{k,l})\varphi(f_{r,s}).$$

所以

$$\mathrm{Aut}D_n=\left\{\begin{bmatrix}1 & 0\\b & a\end{bmatrix}\middle| a\in Z_n^*,b\in Z_n\right\}.$$

点评 本题涉及自同构与同构两个概念，以及如何确定与表达它们. 在计算过程中要有点耐心和细心.

补充题 2-8 证明 $SL(2,\mathbb{Z})$ 可由一个三阶元与一个四阶元生成.

分析 首先搞清 $SL(2,\mathbb{Z})$ 的意义，它是整数元素的行列式为 1 的二阶矩阵所成的群(见例 2.3.1)，可把它具体表达出来，然后找一找其中的三阶元与二阶元，能否由它们生成该群，

证 首先 $SL(2,\mathbb{Z})$ 可表示为

$$SL(2,\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a,b,c,d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

然后在其中取

$$P = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \quad Q = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

则 $P^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$，$P^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$，得 $o(P)=3$. $Q^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$，$Q^4 = I$，得 $o(Q)=4$. 令

$$A = PQ = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \quad B = QP = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

由例 2.3.1 知 $SL(2,\mathbb{Z}) = \langle A,B \rangle$，所以

$$SL(2,\mathbb{Z}) = \langle P,Q \rangle.$$

点评 读者不妨找一下其他的三阶元与一个四阶元.

补充题 2-9 设 p 为素数，$|G| = p^\alpha n_1$，$(p,n_1)=1$. $H \leqslant G$，且 $|H| = p^k$，$1 \leqslant k < \alpha$. 则存在一个子群 N，$|N| = p^{k+1}$，使 $H \lhd N$.

分析 我们可以利用 Sylow 定理，H 被包含在一个 Sylow p-子群 P 里，于是问题变为在 P 里考虑. 可对 α 作归纳法来证明此题.

证 设包含 H 的 Sylow$p$-子群为 P. $|P| = p^\alpha$，$|H| = p^k$，$1 \leqslant k < \alpha$.

对 α 作归纳法. $\alpha=2$，显然结论成立. 下设 $\alpha>2$，且假设结论对小于 α 的情况成立.

由于 p-群有非平凡中心 $C(P)$，可取 p 阶元 $a \in C(P)$，令 $K = \langle a \rangle$，则 $K \lhd P$. 令 $P' = \dfrac{P}{K}$，$H' = \dfrac{H}{K}$，则 $|P'| = p^{\alpha-1}$，$|H'| = p^{k-1}$. 由归纳假设，存在一个子群 N'，$|N'| = p^k$，使 $H' \lhd N'$. 设 $\varphi: P \to \dfrac{P}{K}$ 是自然同态，令 $N = \varphi^{-1}(N')$，则 $H = \varphi^{-1}(H')$，$|N| = p^{k+1}$，且 $H \lhd N$.

因而结论对任何 $\alpha \geqslant 2$ 的正整数都成立.

点评 该题可作为 Sylow 定理的一个补充.

补充题 2-10 设 p 为素数，$|G| = p^\alpha n_1$，$(p,n_1)=1$. H 是 G 的 p-子群，$N_G(H)$ 是 H 的正规化子. 证明 $[G:H] \equiv [N_G(H):H] \pmod p$.

分析 初看起来这个题目不太容易，但从形式上看与 Sylow 定理有关. 我们不妨先看一个例子. 设 $G = S_4$，$|G| = 2^3 3$. $H = \{(1),(12)\}$ 是一个 2-子群. 通过计算可得 $N_G(H) = \{(1),(12),(34),(12)(34)\}$，所以 $[G:H] \equiv [N_G(H):H] \equiv 0 \pmod 2$. 若取 H 为一个 Sylow 2-子群，则由 Sylow 定理的

计数定理可得 $N(p^{\alpha})=[G:N_G(H)]\equiv 1(\text{mod } 2)$，因而等式也成立.

证 设 $|H|=p^k$，按 k 的大小分两种情况讨论.

情况 1：$1\leqslant k<\alpha$，$p\mid[G:H]$，故 $[G:H]\equiv 0(\text{mod } p)$；另一方面，由补充题 2-9，存在一个子群 N，$|N|=p^{k+1}$，使 $H\lhd N$，因而 $H\lhd N\leqslant N_G(H)$，于是有 $[N_G(H):H]=[N_G(H):N][N:H]=p[N_G(H):N]$，故 $[N_G(H):H]\equiv 0(\text{mod } p)$. 所以等式 $[G:H]\equiv[N_G(H):H](\text{mod } p)$ 成立.

情况 2：$k=\alpha$，则 H 是一个 Sylow p-子群，由 Sylow 定理的计数定理，可得 $N(p^{\alpha})=[G:N_G(H)]\equiv 1(\text{mod } p)$，对等式 $[G:H]=[G:N_G(H)][N_G(H):H]$ 的两边作模 p 的运算，得 $[G:H]\equiv[G:N_G(H)][N_G(H):H]\equiv[N_G(H):H](\text{mod } p)$.

点评 该题仍是 Sylow 定理的应用.

补充题 2-11 证明 36 阶群不是单群.

分析 利用 Sylow 定理，方法与例 2.12.2 类似.

证 $|G|=36=2^2 3^2$.

首先看 G 中的 Sylow 3-子群. 由 Sylow 定理，其个数 $N(9)\equiv 1(\text{mod } 3)$. 只有两种情况：$N(9)=1$ 或 4. 当 $N(9)=1$ 时，G 中有惟一的 Sylow 3-子群，因而是正规子群，G 不是单群.

当 $N(9)=4$ 时，有 4 个 Sylow 3-子群. 设 H,K 是两个不同的 Sylow 3-子群，则有

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}=\frac{81}{|H\cap K|},$$

由于 $|HK|\leqslant 36$，故 $|H\cap K|\geqslant 3$.

我们考虑 $N_G(H\cap K)$，由于 $H\cap K\lhd H$，$H\cap K\lhd K$，因而 $\langle H,K\rangle\leqslant N_G(H\cap K)$，故 $|N_G(H\cap K)|>9$，于是可分以下两种情况讨论：

(1) $|N_G(H\cap K)|=18$. 由于 $[G:N_G(H\cap K)]=2$，因而 $N_G(H\cap K)\lhd G$，所以 G 不是单群.

(2) $|N_G(H\cap K)|=36$，则 $H\cap K\lhd G$. 所以 G 不是单群.

点评 本题所用的方法主要是利用子群的正规化子.

补充题 2-12 证明 30 阶群不是单群.

分析 利用 Sylow 定理，方法类似.

证 $|G|=30=2\times 3\times 5$.

首先看 G 中的 Sylow 5-子群. 由 Sylow 定理，其个数 $N(5)\equiv 1(\text{mod } 5)$. 只有两种情况：$N(5)=1$ 或 6. 当 $N(5)=1$ 时，G 中有惟一的 Sylow 5-子群，因而是正规子群，G 不是单群.

当 $N(5)=6$ 时，G 中有 6 个 Sylow 5-子群，设为 $P_1, P_2, \cdots, P_6$，则 $\left|\bigcup_{i=1}^{6} P_i\right| = 5\times6-5=25$. 还剩下 5 个非单位元.

我们再看 G 中的 Sylow 3-子群. 由 Sylow 定理，其个数 $N(3)\equiv1 \pmod 3$. 只有两种情况：$N(5)=1$ 或 4. 因为只剩下 5 个非单位元，不可能有 4 个 Sylow 3-子群，故有惟一的 Sylow 3-子群，因而是正规子群，G 不是单群.

点评 本题主要从分析元素个数来确定有多少个 Sylow 子群.

第3章 环 论

环是建立在群的基础上的有两个运算的代数系，它更接近于我们平时经常在做的加，减，乘，除四则运算的对象，因为四则运算实质上只有两种运算加和乘，减是加的逆运算，除是乘的逆运算．由于群的许多概念与性质可推广到环，所以有许多平行的概念和定理，因此在学习这一章时可以快一些和粗一些．重点放在环与群的不同之处．

3.1 环的基本概念

一、内容提要

1．环$(A,+,\cdot)$的定义

(1)$(A,+)$是加群(可换群)，(2)$(A,\cdot)$是半群，(3)左右分配律成立．加群$(A,+)$中的单位元是零元 0，半群$(A,\cdot)$不一定有单位元，有单位元时把它记作 1．如果乘法可交换，则称为可换环．

一些重要的例：

(1) 数环：$(\mathbb{Z},+,\cdot)$，$(\mathbb{Q},+,\cdot)$，$(\mathbb{R},+,\cdot)$，$(\mathbb{C},+,\cdot)$等．

(2) 整数模 n 的同余类环：$(Z_n,+,\cdot)$．注意：同一个集合 Z_n 既可构成群，也可构成环，要看对什么运算，因此，本书一般都把 Z_n 和运算结合在一起．但有些书同一个符号 Z_n 有时指群，有时指环．读者在看参考书时必须留意．

(3) 数环上添加元素的环：

高斯整数环：$(\mathbb{Z}[i],+,\cdot)$，$\mathbb{Z}[i]=\{a+b\mathrm{i}\mid a,b\in\mathbb{Z},\mathrm{i}=\sqrt{-1}\}$．

可在整数环上添加其他元素：设 $\alpha\in\mathbb{C}\setminus\mathbb{Z}$，$\mathbb{Z}[\alpha]=\{a+b\alpha\mid a,b\in\mathbb{Z}\}$，则它对复数的加法和乘法构成环：$(\mathbb{Z}[\alpha],+,\cdot)$．例如，$(\mathbb{Z}[\sqrt{-3}],+,\cdot)$，$(\mathbb{Z}[\sqrt{-5}],+,\cdot)$，$(\mathbb{Z}[\sqrt{2}],+,\cdot)$，$(\mathbb{Z}[\sqrt{3}],+,\cdot)$等．也可在$\mathbb{Q}$上添加，如$(\mathbb{Q}[\mathrm{i}],+,\cdot)$，$(\mathbb{Q}[\sqrt{2}],+,\cdot)$等．

(4) 全矩阵环：$(M_n(\mathbb{Z}),+,\cdot)$，$(M_n(\mathbb{Q}),+,\cdot)$，$(M_n(\mathbb{R}),+,\cdot)$，$(M_n(\mathbb{C}),+,\cdot)$等．

(5) 多项式环：$(\mathbb{Z}[x],+,\cdot)$，$(\mathbb{Q}[x],+,\cdot)$，$(\mathbb{R}[x],+,\cdot)$等．环 A 上的多项式环$(A[x],+,\cdot)$．多项式环是本章的重点．

(6) 实四元数除环：$H=\{aE+bI+cJ+dK \mid a,b,c,d\in\mathbb{R}\}$，其中 $E=\begin{bmatrix}1&0\\0&1\end{bmatrix}$，$I=\begin{bmatrix}\sqrt{-1}&0\\0&-\sqrt{-1}\end{bmatrix}$，$J=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$，$K=\begin{bmatrix}0&\sqrt{-1}\\\sqrt{-1}&0\end{bmatrix}$.（对比群论里的四元数群，此环是建立在四元数群的基础上的.）H 也可表示为：

$$H=\left\{\begin{bmatrix}a+b\mathrm{i}&c+d\mathrm{i}\\-c+d\mathrm{i}&a-b\mathrm{i}\end{bmatrix}\middle|\,a,b,c,d\in\mathbb{R},\quad \mathrm{i}=\sqrt{-1}\right\}$$

$$=\left\{\begin{bmatrix}u&v\\-\bar{v}&\bar{u}\end{bmatrix}\middle|\,u,v\in\mathbb{C}\right\}.\quad（此表达式容易记忆.）$$

这是一个特殊的例子：它是一个无限的不可交换的除环.

(7) 加群$(G,+)$的自同态环：设 $E(G)=\mathrm{End}(G,+)$是加群 G 上的全体自同态：定义运算$(f\oplus g)(x)=f(x)+g(x)$，$(f\cdot g)(x)=f(g(x))$. 则$(E(G),\oplus,\cdot)$是一个环.

2. 环内一些特殊元素

可逆元(指乘法可逆)，左(右)零因子，零因子等，并有以下性质：

环内无左(右)零因子的充要条件是消去律成立.

3. 环的初等分类

整环：$(A,+,\cdot)$非零，可换，无零因子.

除环：$(A,+,\cdot)$有 0 和 1，$(A^*,\cdot)$是群.（即非零元都可逆.）

域：可换的除环. **有限域**：元素个数有限的域.

4. 若干结果

- $(Z_p,+,\cdot)$是域$\Leftrightarrow p$ 是素数.
- 一个非零的有限无左(右)零因子的环是除环.
- 有限整环是域.

二、习题 3.1 详细解答

3.1-1 设$(A,+,\cdot)$是一个环，在 A^A 中定义$(f\oplus g)(x)=f(x)+g(x)$，$(f\cdot g)(x)=f(x)g(x)$，证明$(A^A,\oplus,\cdot)$是环. 若定义$(f\oplus g)(x)=f(x)+g(x)$，$(f\cdot g)(x)=f(g(x))$，问：$(A^A,\oplus,\cdot)$是否是环？

分析 由于新环是在原来的环上定义，因而采用新的运算符，以示与原环的运算不同. 作为概念题我们必须逐条检验，做得要尽量细一些，不可用"显然"来代替.

证 对第 1 种定义，按环的定义检验如下：

(1) 在$(A^A,\oplus)$中封闭性、结合律成立，单位元是零变换：$O: x \mapsto 0, \forall x \in A$，负元为$(-f)(x)=-f(x)$. 所以$(A^A,\oplus)$是群，且可交换.

(2) 在$(A^A,\cdot)$中封闭性、结合律成立，所以$(A^A,\cdot)$是半群. 有乘法单位元，即单位变换 $e: x \mapsto x, \forall x \in A$.

(3) 分配律：$h(f\oplus g)(x)=h(x)(f\oplus g)(x)=h(x)(f(x)+g(x))=h(x)f(x)+h(x)g(x)=hf(x)+hg(x)=(hf\oplus hg)(x)$，所以 $h(f\oplus g)=hf\oplus hg$. 类似可证右分配律成立.

综上，$(A^A,\oplus,\cdot)$是环.

对第 2 种定义，按环的定义检验如下：

(1) $(A^A,\oplus)$是可换群：同上.

(2) 由群论中的知识，$(A^A,\cdot)$是半群.

(3) 分配律：$h(f\oplus g)(x)=h((f\oplus g)(x))=h(f(x)+g(x))$，不能得出 $h(f(x)+g(x))=hf(x)+hg(x)$，所以分配律不成立.

综上，$(A^A,\oplus,\cdot)$不是环.

点评 在以上验算过程中注意运算符的不同意义，环 A 中的运算记作“$+,\cdot$”，而 A^A 中的运算记作“$\oplus,\cdot$”，照理应将乘法记作$\otimes$，我们偷懒了.

3.1-2 求 Klein 四元群的自同态环的所有元素.

分析 首先应把 Klein 四元群表示成加群形式$(G,+)$，然后求出它的全体自同态 $E(G)=\mathrm{End}G$，最后按自同态环的定义写出$(E(G),\oplus,\cdot)$.

复习加群的自同态环的概念，定义运算恰恰是习题 3.1-1 中第 2 种情况，但对 $\mathrm{End}(G,+)$构成环(见书上例 3.1.6)

解 首先把 Klein 四元群写成加群形式：

$$\begin{aligned} K_4 &= \langle a,b \mid o(a)=o(b)=2, a+b=b+a \rangle \\ &= \{0,a,b,c=a+b\}. \end{aligned}$$

任一 $f\in E(K_4)$满足：$f(0)=0, f(c)=f(a)+f(b)$，因而有以下形式

$$f=\begin{pmatrix} 0 & a & b & c \\ 0 & \alpha & \beta & \alpha+\beta \end{pmatrix},$$

其中 α,β 可取 K_4 中任何元素，所以

$$E(K_4)=\left\{ f_{\alpha\beta}=\begin{pmatrix} 0 & a & b & c \\ 0 & \alpha & \beta & \alpha+\beta \end{pmatrix} \middle| \alpha,\beta\in K_4 \right\},$$

且有$|E(K_4)|=16$.

在 $E(K_4)$中定义加法为$(f\oplus g)(x)=f(x)+g(x)$，乘法为$(f\cdot g)(x)=f(g(x))$. 则$(E(K_4),\oplus,\cdot)$就是 K_4 的自同态环.

点评 该题关键是把加群的全部自同态表达出来. 由该题可构造有限的

非可换环.

3.1-3　证明环$(M_n(\mathbb{Z}),+,\cdot)$中每一左零因子也是右零因子.

分析　$(M_n(\mathbb{Z}),+,\cdot)$是整数元素的全矩阵环.若某个矩阵是左零因子,则它的秩小于n,可利用初等变换将其变形为有一些零行的矩阵,从而易找到一个矩阵左乘为零.

证　设$A,B\in M_n(\mathbb{Z})$满足$AB=\mathbf{0}$,且$A\neq\mathbf{0},B\neq\mathbf{0}$.

由于秩$(A)=r<n$,可用行线性变换即左乘一个可逆阵$C\in M_n(\mathbb{Z})$使

$$CA=\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{r1} & \cdots & a_{rn} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix},$$

(具体过程:可先用有理数做,然后通分后变成整数矩阵.)取

$$D=\begin{bmatrix} 0 & \cdots & 0 & 1 & \cdots & 1 \\ 0 & \cdots & 0 & 1 & \cdots & 1 \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & 1 & \cdots & 1 \end{bmatrix},$$

则

$$DCA=0$$

显然$DC\in M_n(\mathbb{Z})$,且$DC\neq 0$,所以A是右零因子.

点评　一般进行消去法运算会超出整数范围,为什么还能得到整数元素的矩阵呢?

3.1-4　满足$a^2=a$的元素称为幂等元.满足$a^n=0$的元素称为幂零元.证明整环中除零元外无其他的幂零元,除零元和单位元外无其他的幂等元.

分析　首先要复习整环、幂零元和幂等元的概念.

证　(1) 设$a\neq 0,a^n=0,n>1$.由于整环中消去律成立,逐次消去a,可得$a=0$,矛盾,所以不存在非0的幂零元.

(2) 设$a^2=a$.若$a\neq 0$,下面证a必为单位元:由于$\forall x\in A$有$a^2x=ax$,而整环中消去律成立,消去a得$ax=x$,所以a是左单位元.又由于整环是可交换的,所以a是单位元.(为什么不能由$a^2=a$直接消去a?)

点评　在以上的证明过程中实际上可以不用可交换性(为什么?),因此结论对无零因子环成立.即无左(右)零因子环中除零元外无其他的幂零元,除零元和单位元外无其他的幂等元.

3.1-5 设 $\Gamma=\{f(x)\mid[0,1]$上的实连续函数$\}$,定义加法:$(f+g)(x)=f(x)+g(x)$,乘法:$(f\cdot g)(x)=f(x)g(x)$,$x\in[0,1]$.证明:

(1) $(\Gamma,+,\cdot)$是环.

(2) f 是零因子$\Leftrightarrow f(x)$在$[0,1]$上的零点集包含一个开区间.

(3) 求$(\Gamma,+,\cdot)$中的幂零元、幂等元和可逆元.

分析 本题涉及连续函数的性质:两个连续函数的和与积仍是连续函数,满足封闭性,然后很易检验是否满足环的其他条件.

证 (1) 由于两个连续函数的和与积仍是连续函数,满足封闭性.$(\Gamma,+)$中结合律成立,有零元 f_0:$f_0(x)=0$, $\forall x\in[0,1]$.对任何 f 有负元:$-f$.所以$(\Gamma,+)$是群;$(\Gamma,\cdot)$显然是半群;函数的加与乘满足分配律.所以$(\Gamma,+,\cdot)$是环.

(2) $\Rightarrow$:设 $fg=f_0$,且 $f\neq f_0$ 和 $g\neq f_0$,即 $f(x)g(x)=0$, $\forall x\in[0,1]$.由于 $g\neq f_0$,故$\exists x_0\in(0,1)$使 $g(x_0)\neq 0$.根据连续函数性质,存在开区间$(x_0-\varepsilon,x_0+\varepsilon)\subset[0,1]$使 $g(x)\neq 0$, $\forall x\in(x_0-\varepsilon,x_0+\varepsilon)$.因而 $f(x)=0$, $\forall x\in(x_0-\varepsilon,x_0+\varepsilon)$.

$\Leftarrow$:设 $f(x)=0$, $\forall x\in(a,b)$,且 $f\neq f_0$.作连续函数 g 如下:$g(x)\neq 0$, $\forall x\in(a,b)$;$g(x)=0$, $\forall x\in[0,1]\backslash(a,b)$.则 $fg=f_0$,且 $f\neq f_0$ 和 $g\neq f_0$,所以 f 是零因子.

(3) $(\Gamma,+,\cdot)$中的幂零元:由 $f^n=f_0$,得 $f^n(x)=0$, $\forall x\in[0,1]$,因而 $f(x)=0$, $\forall x\in[0,1]$.所以幂零元只有零函数.

在研究幂等元之前我们先研究一下$(\Gamma,+,\cdot)$中是否有单位元.令函数 $f_1(x)=1$, $\forall x\in[0,1]$,是连续函数,故 $f_1\in\Gamma$.由乘法定义$(f_1\cdot f)(x)=f_1(x)f(x)=f(x)$,所以 f_1 是$(\Gamma,+,\cdot)$中的单位元.

幂等元:设 $f^2=f$,得 $f(f-f_1)=f_0$,即 $f(x)(f(x)-1)=0$, $\forall x\in[0,1]$,由函数的连续性得到 $f=f_0$,或 $f=f_1$.所以幂等元有两个:零函数 f_0 和恒等于 1 的函数 f_1.

可逆元:f 可逆$\Leftrightarrow\exists g\in\Gamma$ 使 $fg=f_1\Leftrightarrow f(x)g(x)=1$, $\forall x\in[0,1]\Leftrightarrow f(x)$在$[0,1]$上无零点.

点评 注意在证明过程中利用连续函数的性质.

3.1-6 确定$(M_n(\mathbb{Z}),+,\cdot)$中的幂零元.

分析 首先我们考虑一个非零实 n 阶矩阵,什么情况下若干次方后变成零矩阵?利用线性代数的知识和经验,对角元素为 0 的三角矩阵经过若干次方后就变成了零矩阵.但显然不仅仅是这些矩阵有这样的性质,那么还有哪些矩阵呢?如果一个矩阵通过相似变换能变为对角元素为 0 的上三角矩阵,那

么这个矩阵也是幂零矩阵. 这就与矩阵的特征值和相似标准形有关. 对于实对称矩阵,总与一个对角阵相似,而对于一般的实矩阵可与一个若尔当标准形相似(也许有些同学没有学过若尔当标准形). 因此只要一个矩阵的所有特征值都是 0,则它就与一个对角元素为 0 的上三角矩阵相似 $A\in M_n(\mathbb{Z})$,从而是一个幂零元.

解 设 $A\in M_n(\mathbb{Z})$.

考虑 A 在复数域上的若尔当标准形: 存在可逆阵 $P\in M_n(\mathbb{C})$使

$$PAP^{-1}=\begin{bmatrix}\lambda_1 & * & \cdots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_n\end{bmatrix}=\Lambda.$$

因而有 $PA^kP^{-1}=\Lambda^k, A^k=P^{-1}\Lambda^kP, k\in\mathbb{Z}^+$. 下面证明

$$A^k=0\Leftrightarrow\lambda_1=\cdots=\lambda_n=0.$$

$\Leftarrow$: 显然.

$\Rightarrow$: 反证法: 假设有 $\lambda_i\neq0$,则 $\Lambda^k\neq0$,因而 $A^k\neq0$,矛盾.

综上,得

$(M_n(\mathbb{Z}),+,\cdot)$中的全体幂零元$=\{A\mid A\in M_n(\mathbb{Z})$且 A 在$\mathbb{C}$中的特征值全为 0$\}$.

点评 本题需要较强的线性代数知识.

3.1-7 证明: 环 A 中元素 u 可逆$\Leftrightarrow$(1)存在 v 满足: $uvu=u, vu^2v=1$; 或者(2)存在 v 满足: $uvu=u$,且 v 是惟一满足此条件的元素.

分析 这是环中的元素运算题,可进行加、减、乘(除)运算. 回忆一下在群论中也有一批元素运算题,但在群中只有两种运算. 现在情况要复杂一些.

证 $\Rightarrow$: 设元素 u 可逆. (1)取 $v=u^{-1}$,显然满足 $uvu=u, vu^2v=1$. (2)取 $v=u^{-1}$,显然满足 $uvu=u$,且由 $uvu=u$ 解得 $v=u^{-1}$是惟一确定的.

$\Leftarrow$: (1) 设存在 v 满足: $uvu=u, vu^2v=1$,把 $uvu=u$ 两边右乘 uv 得 $uvu^2v=u^2v$,因而 $u=u^2v$,再两边左乘 v,得 $vu=vu^2v$,故 $vu=1$. 类似可得 $uv=1$. 所以 u 可逆.

(2) 设存在 v 满足: $uvu=u$,且 v 是惟一满足此条件的元素. 任取 $x\in A$,令 $v_1=v-vux-x$,作运算: $uv_1u=uvu+uvuxu-uxu=u+uxu-uxu=u$,由 v 的惟一性,得 $v_1=v$ 和 $vux=x$,由于 x 是任取的,所以 vu 是左单位元. 类似可证 uv 是右单位元. 因而 $vu=vuuv=uv$,所以 vu 是单位元,u 可逆.

点评 其中有一步: 令 $v_1=v-vux-x$,是通过试验得到的,技巧性较高. 读者如发现更加简单的方法请来电告知.

3.1-8 (华罗庚)设 a 和 b 是环中元素,$a,b,ab-1$ 可逆,则 $a-b^{-1}$,$(a-b^{-1})^{-1}-a^{-1}$可逆,且$[(a-b^{-1})^{-1}-a^{-1}]^{-1}=aba-a$.

分析 第 1 问需要作一点变换,而第 2 问只需代入验证即可.

证 由于 $ab-1=(a-b^{-1})b$,两边求逆,得$(a-b^{-1})^{-1}=b(ab-1)^{-1}$.

对第 2 个式子,代入验证:

$$\begin{aligned}[(a-b^{-1})^{-1}-a^{-1}](aba-a)&=(a-b^{-1})^{-1}(a-b^{-1})ba-(ba-1)\\&=ba-ba+1=1.\end{aligned}$$

点评 如果不告诉逆元的答案,我们也可以求:由于

$$(a-b^{-1})^{-1}-a^{-1}=(a-b^{-1})^{-1}[1-(a-b^{-1})a^{-1}]=(a-b^{-1})^{-1}b^{-1}a^{-1},$$

两边求逆,得$[(a-b^{-1})^{-1}-a^{-1}]^{-1}=ab(a-b^{-1})=aba-a$.

***3.1-9** 证明:$a,b\in A,1-ab$ 可逆$\Rightarrow 1-ba$ 可逆.

分析 这是个打星号题,有难度,初看起来好像无从下手. 首先环 A 是一个有单位元 1 的一般环. 已知 $1-ab$ 可逆,要证 $1-ba$ 可逆. 只能从逆元的定义出发,设 $1-ba$ 的逆元为 u,则有$(1-ba)u=1$. 如何求逆元 u 呢? 有两条思路,一是利用前一题的结果,先把 $a,b,ab-1$ 都看作可逆,然后由上题结果用$(1-ab)^{-1}$表出$(1-ba)^{-1}$,并设法消去式中的 a^{-1} 和 b^{-1}. 另一条思路是借助其他方法找出$(1-ba)^{-1}$的表达式. 我们用两种方法都做一做.

方法 1 先把 $a,b,ab-1$ 都看作可逆,由上题结果得

$$\begin{aligned}[(a-b^{-1})^{-1}-a^{-1}]^{-1}=aba-a\Rightarrow&[a^{-1}-(a-b^{-1})^{-1}]^{-1}\\&=a-aba=a(1-ba).\end{aligned}$$

由于左边可逆,右边也可逆,两边求逆,得

$$(1-ba)^{-1}=[a^{-1}-(a-b^{-1})^{-1}]a,$$

经整理后可得

$$(1-ba)^{-1}=1+b(1-ab)^{-1}a.$$

但以上的结果是在增加了一些假设(a,b 都看作可逆)才得到的,但在后面的证明中没有这个要求了.

方法 2 为了得到$(1-ba)^{-1}$的表达式,我们利用数学分析中的级数展开,在环中定义形式级数:

$$(1-u)^{-1}=\frac{1}{1-u}=1+u+u^2+\cdots,$$

于是有

$$(1-ba)^{-1}=\frac{1}{1-ba}=1+ba+(ba)^2+\cdots$$

$$=1+b(1+ab+(ab)^2+\cdots)a$$
$$=1+b(1-ab)^{-1}a.$$

以上分析过程可在草稿纸上进行,写出证明只需以下简单几行.

证 对元素 $1+b(1-ab)^{-1}a$ 进行以下运算:

$$\begin{aligned}(1-ba)[1+b(1-ab)^{-1}a] &= (1-ba)+(1-ba)b(1-ab)^{-1}a \\ &= (1-ba)+(b-bab)(1-ab)^{-1}a \\ &= (1-ba)+b(1-ab)(1-ab)^{-1}a \\ &= 1-ba+ba = 1.\end{aligned}$$

所以 $1-ba$ 可逆,且有

$$(1-ba)^{-1} = 1+b(1-ab)^{-1}a.$$

点评 分析中方法 1 与方法 2 的共同特点是先用某种方法求出 $(1-ba)^{-1}$ 的表达式,然后加以证明. 可以把求 $(1-ba)^{-1}$ 的表达式的过程隐去,直接计算 $(1-ba)[1+b(1-ab)^{-1}a]$,从而证明 $1-ba$ 可逆.

3.1-10 设 u 有右逆元,证明以下命题等价:

(1) u 有多于一个右逆元;

(2) u 不是可逆元;

(3) u 是左零因子.

分析 这显然是在不可交换环里讨论问题,涉及逆元、零因子等概念. 直观上看,这几个命题都表明元素不可逆. 证明方法用循环证法.

证 (1)⇒(2):设 u 有两个不同的右逆元 v_1, v_2,则 $uv_1=uv_2=1$,若 u 是可逆元,则左乘 u^{-1} 得 $v_1=v_2=u^{-1}$,矛盾. 所以 u 不是可逆元.

(2)⇒(3):由于题设 u 有右逆元,设为 v,则 $uv=1$. 由于 u 不是可逆元,因而 $vu\neq1$. 于是 $uv=1\Rightarrow uvu=u\Rightarrow u(vu-1)=0$. 由于 $(vu-1)\neq0$,所以 u 是左零因子.

(3)⇒(1):设 u 是左零因子,因而有 $w\neq0$ 使 $uw=0$. 又由于题设 u 有右逆元,设为 v,则 $uv=1$. 令 $v_1=v+w$,则 v_1 也是右逆元,且 $v_1\neq v$. 所以 u 有多于一个右逆元.

点评 通过该题可以了解到环中元素是否可逆与是否是零因子是有联系的.

***3.1-11** (Kaplansky)如果环中一个元素有多于一个右逆,则有无穷多个右逆.

分析 首先与上一题有关,由上一题的证明中,已给出一个构造的方法,但如何由两个右逆构造出无穷多个右逆还需想办法.

证 设 u 有多于一个右逆,首先由上题结果,得到 u 不可逆.

设元素 u 有右逆 v_1：$uv_1=1$，因为 u 不可逆，$v_1u\neq 1$，令

$$v_{k+1}=v_1+v_ku-1,\quad k=1,2,\cdots.$$

首先我们证明它们都是 u 的右逆，且互不相同.

对 k 作归纳法. $k=1$，$v_2=v_1+v_1u-1$，两边左乘 u，得 $uv_2=uv_1+uv_1u-u=1+u-u=1$，所以 v_2 是 u 的右逆.

$$v_2=v_1+v_1u-1\Rightarrow v_2-v_1=v_1u-1\neq 0\Rightarrow v_2\neq v_1.$$

假设结论对 $k<n$ 都成立，要证结论对 $k=n$ 也成立. 由于

$v_{n+1}=v_1+v_nu-1$，两边左乘 u，得 $uv_{n+1}=uv_1+uv_nu-u$，由归纳假设，得 $uv_{n+1}=uv_1+uv_nu-u=1+u-u=1$，故 v_{n+1} 是 u 的右逆.

由于 $v_{n+1}=v_1+v_nu-1$，首先显然有 $v_{n+1}-v_1=v_nu-1\neq 0$，因而 $v_{n+1}\neq v_1$. 进一步，对任何 i：$1\leqslant i<n$，$v_{i+1}=v_1+v_iu-1$ 有 $v_{n+1}-v_{i+1}=(v_n-v_i)u$. 如果 $v_{n+1}-v_{i+1}=0$，则 $(v_n-v_i)u=0$，右乘 v_1，得 $(v_n-v_i)=0$，即 $v_n=v_i$，与归纳假设矛盾.

这就证明了 v_k，$k=1,2,\cdots$ 互不相同. 所以结论对 $k=n$ 成立.

综上，u 有无穷多个右逆.

点评 该题说明当某个元素有多个右逆元时，该环必为无限环，也就是说，在有限环内不可能存在某个元素有多于一个右逆元.

是否有不同的构造方法来证明此题，请读者自己思考.

3.1-12 D 是整环，则 $D[x]$ 也是整环.

分析 复习整环概念，逐条检验即可.

证 D 是整环 $\Rightarrow D\neq\{0\}\Rightarrow D[x]\neq\{0\}$.

D 可交换，显然 $D[x]$ 也可交换.

D 内无零因子. 下证 $D[x]$ 内也无零因子：$\forall f(x),g(x)\in D[x]^*$，设 $\deg f(x)=n\geqslant 0$，$\deg g(x)=m\geqslant 0$. 若 $f(x)g(x)=0$，则左边有 $\deg f(x)g(x)=n+m\geqslant 0$，而右边的零多项式不定义次数. 所以矛盾. 因此 $D[x]$ 内无零因子.

综上，$D[x]$ 是整环.

点评 注意对零多项式不定义次数，只对非零多项式定义次数，并有公式

$$\forall f(x),g(x)\in D[x]^*,\quad \deg f(x)g(x)=\deg f(x)+\deg g(x).$$

3.2 子环、理想和商环

一、内容提要

子环、理想和商环是与群论中的子群、正规子群和商群相对应的概念，因此只需注意环的特点，就可轻松掌握.

1. 子环

设$(A,+,\cdot)$是环.

- 概念：$S\subseteq A$，$(S,+,\cdot)$也是环，称S是A的子环，也记作$S\leqslant A$. $\{0\}$与A称为平凡子环.
- 非空子集S是A的子环的条件：$\forall a,b\in S$有$a-b,ab\in S$，则$S\leqslant A$.
- 环内子集的运算：设$S,T\subseteq A$，

$$S+T=\{a+b\mid a\in S,b\in T\},$$
$$ST=\left\{\sum ab\mid a\in S,b\in T\right\},$$

特别注意子集乘积的定义除了元素乘积，还包括元素乘积的和.

- 子环的运算：$S,T\leqslant A\Rightarrow S\cap T\leqslant A$. 注意：$S+T$和$ST$不一定是子环.
- 生成子环：设S是A的非空子集，则包含S的最小子环称为S的生成子环，记作$[S]$. 一个元素的生成子环可表示为：$[a]=\left\{\sum n_k a^k\mid n_k\in\mathbb{Z},k\in\mathbb{Z}^+\right\}$.

2. 理想

理想的概念与群论中的正规子群的概念类似.

设$I\leqslant A$，若$\forall a\in I$和$\forall x\in A$有$xa\in I$(或$AI\subseteq I$)，则称I是A的左理想；若$\forall a\in I$和$\forall x\in A$有$ax\in I$(或$IA\subseteq I$)，则称I是A的右理想；既是左理想又是右理想称为理想. $\{0\}$，A称为平凡理想.（在数学中极少采用像“理想”这样的人文名词作为数学名词，究竟何来？需从当初的历史中发现其奥秘.）

子环与理想的根本区别在于：子环只与内部的元素有关，而理想不仅与内部的元素有关而且与外部的元素有关.（对比子群与正规子群.）

- 子集I是A的理想的条件：$\forall a,b\in I$，$\forall x\in A$有$a-b,xa,ax\in I$.
- 理想的运算：

  (1) I,J是理想$\Rightarrow I\cap J,I+J,IJ$都是理想.

  (2) I是理想，S是子环$\Rightarrow I\cap S$是理想，$I+S$是子环.

  (3) A是有1的环，I是理想，则$1\in I\Rightarrow I=A$.
- 生成理想：设S是A的非空子集，则包含S的最小理想称为S的生成理想，记作(S). 一个元素的生成理想可表示为：$(a)=\left\{\sum xay+sa+at+na\mid x,y,s,t\in A,n\in\mathbb{Z}\right\}$.

当A可交换时，$(a)=\{xa+na\mid a\in A,n\in\mathbb{Z}\}$.

当A可交换且有单位元1时，$(a)=\{xa\mid a\in A\}=aA$，且$(1)=A$.

由一个元素生成的理想称为主理想，以后我们将专门讨论.

- **单环**：不含非平凡理想的环称为单环. 除环与域都是单环. 数域 F 上的全矩阵环$(M_n(F),+,\cdot)$是单环.
- **极大理想及其性质**：设 A 是一个环，若 M 是 A 的一个非平凡理想，且没有真包含 M 的非平凡理想，则称 M 是 A 的一个极大理想. 有以下性质：

  设 M 是 A 的一个理想，则 M 是 A 的极大理想$\Leftrightarrow A/M$ 是单环.

  设 A 可交换且有单位元，则 M 是 A 的一个极大理想$\Leftrightarrow A/M$ 是域.
- **素理想及其性质**：设环 A 可交换，P 是 A 的一个非平凡理想，若满足：$ab\in P\Rightarrow a\in P$ 或 $b\in P$，则称 P 是 A 的一个素理想. 有以下性质：

设环 A 可交换，则 P 是 A 的一个素理想$\Leftrightarrow A/P$ 是整环.

(为什么称为素理想呢？因为它和素数有某种相似和联系，素数 p 满足：$p|ab\Rightarrow p|a$ 或 $p|b$. 在$(\mathbb{Z},+,\cdot)$中素数 p 生成的理想(p)就是素理想.)

3. 商环

环 A 对理想 I 的加法陪集关于陪集的加法和乘法运算所成的环，称为 A 模理想 I 的商环(同余类环)，记作 $A/I=\{a+I\,|\,a\in A\}$. 且有

$$a+I=b+I\Leftrightarrow a\equiv b(\mathrm{mod}\ I).$$

虽然概念比较多，但许多概念与群的概念类似，我们一开始重点在于理解，不必企图马上都记住，等以后用到时再查阅，逐步加深印象.

4. 若干结果

- $(\mathbb{Z},+,\cdot)/(n)=(Z_n,+,\cdot)$.
- 设 p 是素数，$p\nmid n$，则 $p^{\varphi(n)}\equiv 1(\mathrm{mod}\ n)$.

二、习题 3.2 详细解答

3.2-1 设 S 是环 A 的非空子集，证明 S 是 A 的子环的充分必要条件是对任意 $a,b\in S$ 有 $a-b\in S$ 和 $ab\in S$.

分析 这是一个检验题，必须像例行公事一样，逐条检验.

证 必要性：显然.

充分性：对任意 $a,b\in S$ 有 $a-b\in S$，由群的理论得$(S,+)$是子群. 对任意 $a,b\in S$ 有 $ab\in S$，知$(S,\cdot)$是半群. S 中分配律自然成立.

所以 S 是 A 的子环.

点评 虽然证明非常简单,但每一步都要思考一下.

3.2-2 设 S_1, S_2 是 A 的子环,则 $S_1 \cap S_2$ 也是 A 的子环. S_1+S_2 也是子环吗?

分析 可利用习题 3.2-1 中的条件来检验. 第 2 问,查一下内容提要,没有这一定理,可以断定不成立,要证明命题不成立的方法是举出反例.

证 由上题子环的充分必要条件,要证对任意 $a, b \in S_1 \cap S_2$,有 $a-b \in S_1 \cap S_2$ 和 $ab \in S_1 \cap S_2$. 因为 S_1, S_2 是 A 的子环,故 $a-b \in S_1$ 和 $a-b \in S_2$,因而 $a-b \in S_1 \cap S_2$. 类似 $ab \in S_1 \cap S_2$,所以 $S_1 \cap S_2$ 是子环.

S_1+S_2 不一定是子环,主要是对任意 $a, b \in S_1+S_2$,不一定有 $ab \in S_1+S_2$.

在矩阵环中很容易找到反例:设 $A=M_2(\mathbb{Z})$, $S_1=\left\{\begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \middle| a, c \in \mathbb{Z}\right\}$, $S_2=\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle| a, b \in \mathbb{Z}\right\}$,易见 S_1, S_2 是 A 的子环,但 $S_1+S_2=\left\{\begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \middle| a, b, c \in \mathbb{Z}\right\}$不是子环.

点评 对第 2 问的反例只有在子环不是理想的环中找. 读者试在其他环中找一个反例.

3.2-3 设 H 是环 A 的非空子集,证明 H 是 A 的理想的充分必要条件是对任意 $a, b \in H$ 和 $\forall x \in A$ 有 $a-b, xa, ax \in H$.

分析 该题与习题 3.2-1 类似,没有任何难度.

证 必要性:显然.

充分性:因对任意 $a, b \in H$ 有 $a-b, ab \in H$,所以 H 是子环. 又因对任意 $a \in H$ 和 $\forall x \in A$ 有 $xa, ax \in H$. 所以 H 是理想.

点评 一般情况下,要先证明 H 是子环,再证 H 是理想. 今后有了本题的结论,就不用分两步走了.

3.2-4 I, J 是理想 $\Rightarrow I \cap J, I+J, IJ$ 都是理想. 并在$(\mathbb{Z}, +, \cdot)$中确定 $(m) \cap (n)$, $(m)+(n)$, $(m)(n)$.

分析 利用上一题的条件进行检验.

证与解 根据上一题的条件,对任意 $a+u \in I, b+v \in J$ 有 $(a+u)-(b+v)=(a-b)+(u-v) \in I+J$. 又 $\forall x \in A$ 有 $x(a+u)=xa+xu \in I+J$, $(a+u)x=ax+ux \in I+J$,所以 $I+J$ 是理想.

由乘法定义，$IJ=\left\{\sum au \mid a\in I,u\in J\right\}$. 对任意$\sum au,\sum bv\in IJ$有$\sum au-\sum bv=\sum au+(-b)v\in IJ$，又$\forall x\in A$有$x\sum au=\sum xau=\sum a'u\in IJ$，类似有$(\sum au)x\in IJ$. 所以$IJ$是理想.

类似可证$I\cap J$是理想.（略）

由群论中的结论，$(\mathbb{Z},+,\cdot)$中的全部子加群为$\{qn\mid q\in\mathbb{Z}\}$，$n=0,1,2,\cdots$. 因而可设

$$(m)\cap(n)=(r),\quad (m)+(n)=(d),\quad (m)(n)=(s).$$

(1) $(m)\cap(n)=(r)$，则$r=qm=hn$，r是m和n的公倍数，故$r\in([m,n])$. 另一方面，$[m,n]\in(m)\cap(n)=(r)$. 所以$r=[m,n]$.

(2) $(m)+(n)=(d)$，则$d=sm+tn$，故$d\in((m,n))$，$(m,n)\mid d$；另一方面，由最大公因子定理，$(m,n)=am+bn\in(m)+(n)=(d)$，$d\mid(m,n)$. 所以$d=(m,n)$.

(3) $(m)(n)=(s)$，则$s=qmn$. 另一方面，$mn\in(s)$，$s\mid mn$. 所以$s=mn$.

点评 该题要仔细做，对理想的运算加深印象. 可对比群论中的类似结果.

3.2-5 确定$(Z_n,+,\cdot)$中的所有理想.

分析 由于环中的理想就是其加群$(Z_n,+)$中的子群，而$(Z_n,+)$中的全部子群我们已知道（见习题 2.2-3 的习题解答）：

$(Z_n,+)$的全部子群为$N_m=\{k\bar{m}\mid k\in\mathbb{Z}\}$，其中$m=0$，或$0<m<n$且$m\mid n$.

解 由于$(Z_n,+,\cdot)$中的理想就是$(Z_n,+)$的子群，而$(Z_n,+)$的全部子群为

$$N_m=\{k\bar{m}\mid k\in\mathbb{Z}\},\quad \text{其中 } m=0,\quad \text{或 } 0<m<n \text{ 且 } m\mid n.$$

经检验，它们都是$(Z_n,+,\cdot)$中的理想，所以$(Z_n,+,\cdot)$中的所有理想为

$$N_m=\{k\bar{m}\mid k\in\mathbb{Z}\},\quad \text{其中 } m=0,\quad \text{或 } 0<m<n \text{ 且 } m\mid n.$$

点评 对于那些与群相同的对象，可以利用群中的结果.

3.2-6 证明$(M_n(\mathbb{Z}),+,\cdot)$不是单环，并确定$(M_n(\mathbb{Z}),+,\cdot)$中的所有理想.

分析 主教材 3.2 节曾证明了数域F上的全矩阵环$(M_n(F),+,\cdot)$是单环. 它们的区别在于矩阵元素的取值范围，数域F是单环，而整数环$\mathbb{Z}$不是单环，即$\mathbb{Z}$中有非平凡理想. 这就使我们想到，如果矩阵取值在$\mathbb{Z}$的理想里，则对应的$M_n(\mathbb{Z})$中的子环可能也是理想.

证 整数环$(\mathbb{Z},+,\cdot)$有理想：(d)，$d=0,1,2,\cdots$. 因而我们猜想$(M_n(F),+,\cdot)$中全部理想为

$$I_d = \{(a_{ij})_{n\times n} \mid a_{ij} \in (d)\}, \quad d = 0,1,2,\cdots. \qquad (*)$$

下面我们来证明这一点.

首先,I_d 显然是理想.

再证明$(M_n(\mathbb{Z}),+,\cdot)$中任何一个理想都是某个 I_d:

设 J 是$M_n(\mathbb{Z})$中任何一个理想.令

$$H = \{a \mid a \text{ 是矩阵 } A \in J \text{ 中的元素}\},$$

即 H 是 J 中所有矩阵的元素所构成的集合,因而 H 是$\mathbb{Z}$的子集.可证 H 是$(\mathbb{Z},+,\cdot)$的一个理想:

对于任何 $a_{ij},b_{kl}\in H$,设 a_{ij} 是矩阵 $A\in J$ 中的第(i,j)个元素,b_{kl} 是矩阵 $B\in J$ 中的第(k,l)个元素,则 $E_{ii}AE_{jj}-E_{ik}BE_{lj}=(a_{ij}-b_{kl})E_{ij}\in J$,所以 $a_{ij}-b_{kl}\in H$.其中 E_{ij} 是第(i,j)个元素为 1,其余元素为 0 的矩阵.又对于任何 $a_{ij}\in H$,$\forall x\in\mathbb{Z}$,有 $xA,Ax\in J$,故 $xa_{ij},a_{ij}x\in H$.

所以 H 是$(\mathbb{Z},+,\cdot)$的一个理想.

这就证明了$(M_n(\mathbb{Z}),+,\cdot)$中全部理想为$(*)$.

点评 注意不仅仅给出结果,要加以证明.

3.2-7 设 L 是 A 的左理想,则 L 的左零化子 $N=\{x\mid x\in A,xL=0\}$是 A 的一个理想.

分析 按条件检验.

证 按理想的条件来证.

对任意 $a,b\in N$,由于$(a-b)L=aL-bL=0$,故 $a-b\in N$.

对任意 $a\in N$,$\forall x\in A$ 有 $xaL=0$,$axL=aL=0$,故 $xa,ax\in N$.

所以 N 是 A 的理想.

点评 可以对右理想作出类似的结果.

3.2-8 设 A 是环,H 是理想,决定 A/H:

(1) $A=(\mathbb{Z}[x],+,\cdot)$,$H=(x^2+1)$;

(2) $A=(\mathbb{Z}[i],+,\cdot)$,$H=(2+\mathrm{i})$;

(3) $A=\left\{\begin{bmatrix} a & b \\ 0 & c\end{bmatrix}\middle| a,b,c\in\mathbb{Z}\right\}$, $H=\left\{\begin{bmatrix} 0 & 2x \\ 0 & 0\end{bmatrix}\middle| x\in\mathbb{Z}\right\}$.

分析 这是一个计算题,要求把商环的元素表达出来,先按商环的定义写出,然后看是否能表达得尽量简单.

解 根据商环的定义,其元素是加群中的陪集.

(1) 按商环的定义可得

$A/H=\mathbb{Z}[x]/(x^2+1)=\{ax+b+(x^2+1)\mid a,b\in\mathbb{Z}\}=\{\overline{ax+b}\mid a,b\in\mathbb{Z}\}$.

点评 进一步可证(学了 3.3 节后)：$\mathbb{Z}[x]/(x^2+1)\cong\mathbb{Z}[\mathrm{i}]$.

(2) 按定义可写出

$A/H=\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})=\{a+b\mathrm{i}+(2+\mathrm{i})\mid a,b\in\mathbb{Z}\}=\{\overline{a+b\mathrm{i}}\mid a,b\in\mathbb{Z}\}$.

但此表达式太一般了，我们可进一步把它的元素表达得更简单一些. 我们来看此商环有哪些元素？由于$\overline{2+\mathrm{i}}=\overline{0}$，得 $\overline{\mathrm{i}}=\overline{-2}$，因此有可将每一个陪集的代表元变为整数：$\overline{a+b\mathrm{i}}=\overline{a-2b}$. 又因 $5=(2+\mathrm{i})(2-\mathrm{i})$，得到 $\overline{5}=\overline{0}$，所以$\dfrac{\mathbb{Z}[\mathrm{i}]}{(2+\mathrm{i})}$中只有 5 个元素：$\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}$. 于是

$$\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}.$$

其中 $\overline{k}=k+(2+\mathrm{i}),k=1,2,\cdots,5$.

点评 由于 5 个元素的加群只有$(Z_5,+)$，我们把群的同构推广到环，显然有$\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})\cong(Z_5,+,\cdot)$. 关于环的同构的概念将在下一节给出，到时可严格证明.

(3) $A=\left\{\begin{bmatrix}a & b\\0 & c\end{bmatrix}\middle| a,b,c\in\mathbb{Z}\right\}$，$H=\left\{\begin{bmatrix}0 & 2x\\0 & 0\end{bmatrix}\middle| x\in\mathbb{Z}\right\}$.

我们先来看加群的陪集是什么样的元素. 由于对任何$\begin{bmatrix}a & b\\0 & c\end{bmatrix}\in A$，可表示为

$$\begin{bmatrix}a & b\\0 & c\end{bmatrix}=\begin{bmatrix}a & 0\\0 & c\end{bmatrix}+\begin{bmatrix}0 & 2n\\0 & 0\end{bmatrix},\quad 当\ b=2n\ 时,$$

$$\begin{bmatrix}a & b\\0 & c\end{bmatrix}=\begin{bmatrix}a & 1\\0 & c\end{bmatrix}+\begin{bmatrix}0 & 2n\\0 & 0\end{bmatrix},\quad 当\ b=2n+1\ 时.$$

所以得

$$A/H=\left\{\overline{\begin{bmatrix}a & 0\\0 & c\end{bmatrix}},\overline{\begin{bmatrix}a & 1\\0 & c\end{bmatrix}}\middle| a,c\in\mathbb{Z}\right\}.$$

点评 虽然商环一般可表示为 $A/H=\{a+H\mid a,c\in\mathbb{Z}\}=\{\overline{a}\mid a\in A\}$，但对于具体的商环应表示得尽量简单.

3.2-9 设 F 是数域，则(x)是 $F[x]$的极大理想，从而 $F[x]/(x)$是域.

分析 先复习极大理想的概念.

证 先证(x)是极大理想. 根据极大理想的定义，首先要证它是非平凡理想：显然$(x)\neq 0$ 和$(x)\neq F[x]$，所以(x)是非平凡理想.

其次要证，若有理想 I 真包含(x)，则必有 $I=F[x]$：因为 I 真包含(x)，则存在 $f(x)\in I\setminus(x)$，设 $f(x)=a_0+a_1x+\cdots+a_nx^n$，由于 $f(x)\notin(x)$，故

$a_0 \neq 0$. 由此可得 $a_0 = f(x) - x(a_1 + \cdots + a_n x^{n-1}) \in I$,于是 $a_0 \in I, a_0^{-1} a_0 = 1 \in I$,故 $I = F[x]$.

所以(x)是极大理想.

再由教材中的定理 3.2.1 知 $F[x]/(x)$是域.

点评 与群论中的极大正规子群类似,可讨论找出某些环中的所有极大理想问题. 例如,找出$(\mathbb{Z}, +, \cdot)$,$F[x]$中的所有极大理想.

3.2-10 设 D 为有单位元的环,则 D 为除环的充分必要条件是 D 没有非平凡左理想.

分析 我们要反复复习整环、除环和域等概念,本题只需从概念出发进行证明.

证 除环的定义:环中有 1,对任何非零元有逆元.

必要性:设 I 为非零左理想,则存在 $a \in I, a \neq 0$. 因 I 是左理想,取 $a^{-1} \in D$ 得 $a^{-1}a = 1 \in I$,所以 $I = D$. 所以 D 中没有非平凡左理想.

充分性:已知 D 没有非平凡左理想,要证 D 是除环.

任取 $a \in D^*$,则 Da 是一个左理想(为什么?),因为 $a \in Da$,故 $Da \neq 0$. 由于 D 没有非平凡左理想,故必有 $Da = D$, 于是存在 $b \in D$ 使 $ba = 1$,故 a 有左逆元,由此可得 D^* 是群,所以 D 是除环.

点评 在证明过程中有些细节要多问几个为什么,以达到复习的目的.

3.2-11 设 R 是可换环,H 是理想,且 $H \neq R$,则 H 是素理想的充分必要条件是 R/H 是整环. 素理想的定义为:设环 A 可交换,P 是 A 的一个非平凡理想,若满足:$ab \in P \Rightarrow a \in P$ 或 $b \in P$,则称 P 是 A 的一个素理想.

分析 素理想的概念不易记忆,可与素数的概念相比较,形式上有某种类似性:

素数满足:$p = ab \Rightarrow p \mid a$ 或 $p \mid b$.

素理想满足:$ab \in P \Rightarrow a \in P$ 或 $b \in P$.

证 必要性:已知 H 是素理想,要证 $R/H = \{a + H \mid a \in R\}$是整环. 只需证明 R/H 中无零因子.

设 $\bar{a} = a + H \in R/H$(模 H 的同余类). 若有 $a, b \in R$ 满足 $\bar{a}\,\bar{b} = \bar{0}$. 由于 $\bar{a}\,\bar{b} = (a + H)(b + H) = ab + H = \bar{0} = H$,故得 $ab \in H$. 由于 H 是素理想,得到 $a \in H$ 或 $b \in H$,因而有 $\bar{a} = \bar{0}$ 或 $\bar{b} = \bar{0}$,所以 R/H 内无零因子,因而是整环.

充分性:已知 R/H 是整环,要证 H 是素理想.

设 $ab \in H$, 则 $\bar{a}\,\bar{b} = \bar{0}$,因 R/H 是整环,故有 $\bar{a} = \bar{0}$ 或 $\bar{b} = \bar{0}$,即 $a \in H$ 或 $b \in H$,所以 H 是素理想.

点评 这是概念题，必须对照定义来证.

3.3 环的同构与同态

一、内容提要

环的同构与同态完全是群的同构与同态概念的推广，只要注意环中有两种运算，因而要保持两种运算，群的同构与同态的一系列定理都可推广到环中.

1. 环的同态与同构的概念

两个环之间的同态(构)映射就是保持运算的映(双)射.

- **环的同态**：设$(A,+,\cdot)$，$(A',\oplus,\times)$是两个环，映射 $f:A\to A'$满足(保持运算)：

$$f(a+b)=f(a)\oplus f(b) \quad 和 \quad f(ab)=f(a)\times f(b),$$

则称 f 是$(A,+,\cdot)$到$(A',\oplus,\times)$的同态(映射).

- $f(0)=0'$，$f(na)=nf(a)$，$n\in\mathbb{Z}$；$f(a^n)=(f(a))^n$，$n\in\mathbb{Z}^+$.
- 子环 $H\leqslant A\Rightarrow f(H)\leqslant A'$，特别是 $f(A)\leqslant A'$；理想 $I\lhd A\Rightarrow f(I)\lhd f(A)$.（为方便起见，本书采用子群的记号表示子环，用正规子群的记号表示理想.）
- 零同态：$\theta(x)=0'$，$\forall x\in A$.
- 当 f 是双射，则称 f 是同构，记作 $A\cong A'$.
- 当 f 是单射，称 f 是单同态，这时 $A\cong f(A)$.
- 当 f 是满射，即 $f(A)=A'$，称 f 是满同态，这时记作 $A\overset{f}{\sim}A'$.（注意用记号：$\overset{f}{\sim}$表示满同态，非满同态不能用此记号.）
- 同态核：$\ker f=\{a\in A\mid f(a)=0'\}\lhd A$. 同态核是非常重要的概念.
- f 是单同态$\Leftrightarrow\ker f=0$.
- $A\overset{f}{\sim}A'$，则 f 是同构$\Leftrightarrow\ker f=0$.
- 同态的全原像：$f(a)=a'\Rightarrow f^{-1}(a')=a+\ker f$. $H'\leqslant f(A)\Rightarrow f^{-1}(H')\leqslant A$，$I'\lhd f(A)\Rightarrow f^{-1}(I')\lhd A$. $f(H)=H'\Rightarrow f^{-1}(H')=H+\ker f$.
- 自同态：$f:A\to A$，$\forall x\in A$. 单位同态：$f(x)=x$，$\forall x\in A$.

2. 有关环的同态与同构的定理

- **同态基本定理**：$f:A\to A'$是满同态，$K=\ker f$，则(1)存在同构 σ：$A/K\overset{\sigma}{\cong}$

A',(2) $\varphi(a)=a+K$ $(A\to A/K)$(称 φ 为 A 到其商环的**自然同态**),并有

$$f=\sigma\varphi.$$

- **子环(理想)对应定理**:设 $A\overset{f}{\sim}A'$,$K=\ker f$,$S=\{H\mid K\leqslant H\leqslant A\}$,$T=\{N\mid N\leqslant A'\}$,则存在双射 $\tau:H\mapsto f(H)(S\to T)$.
- **商环同构定理**:设 $A\overset{f}{\sim}A'$,$K=\ker f$,$K\leqslant I\lhd A$,则
$$A/I\cong A'/f(I)\cong\frac{A/K}{I/K}.$$
- **第二同构定理**:$I\lhd A$,$H\leqslant A$,则
$$(H+I)/I\cong H/(H\cap I).$$
- **利用同态基本定理证明某些环的同构的方法**:证明 $\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})\cong(Z_5,+,\cdot)$.

首先我们来建立一个 $(\mathbb{Z}[\mathrm{i}],+,\cdot)$ 到 $(Z_5,+,\cdot)$ 的满同态 f,并使 $\ker f=(2+\mathrm{i})$,则可得证. 设 $f:\mathbb{Z}[\mathrm{i}]\to(Z_5,+,\cdot)$ 是满同态,则应有 $f(1)=\bar{1}$. 由于 $f(a+b\mathrm{i})=\bar{a}+\bar{b}f(\mathrm{i})$,元素 i 的像决定了 f. 又由于 $f(\mathrm{i})f(\mathrm{i})=f(-1)=-1=4(\mathrm{mod}5)$,所以得 $f(\mathrm{i})=\pm2$. 取 $f(\mathrm{i})=-2$,则得 $f(a+b\mathrm{i})=\bar{a}-2\bar{b}$,易验证 f 保持运算. f 的核为

$$\begin{aligned}\ker f&=\{a+b\mathrm{i}\mid a-2b\equiv0(\mathrm{mod}\ 5)\}=\{b(2+\mathrm{i})+5n\mid n\in\mathbb{Z}\}\\&=(2+\mathrm{i}),\end{aligned}$$

所以由同态基本定理得到 $\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})\cong(Z_5,+,\cdot)$. 证毕.

3. 整环的分式域

设 D 是整环,则存在包含 D 的分式域:

$$P(D)=\left\{\frac{b}{a}\,\middle|\,a\in D^*,b\in D\right\}.$$

二、习题 3.3 详细解答

3.3-1 设 f 是环 A 到 A' 的同态,证明:

(1) f 将 A 中的 0 元映成 A' 中的 $0'$ 元;

(2) f 将 A 中的子环映成 A' 中的子环;

(3) f 将 A 中的理想映成 $f(A)$ 中的理想.

分析 这是概念题,认真复习概念.

证 (1) 由同态定义,$f(0)=f(0+0)=f(0)+f(0)$,所以 $f(0)=0'$.

(2) 设 H 是子环,对于任意 $f(h_1),f(h_2)\in f(H)$ 有

$$f(h_1)-f(h_2)=f(h_1-h_2)\in f(H),$$
$$f(h_1)f(h_2)=f(h_1h_2)\in f(H),$$

所以 $f(H)$是子环.

(3) 设 I 是 A 的理想,由(2)得 $f(I)$是子环.

对于任意 $f(a)\in f(I), f(x)\in f(A)$有

$$f(x)f(a)=f(xa)\in f(I),$$
$$f(a)f(x)=f(ax)\in f(I),$$

所以 $f(I)$是 $f(A)$的理想.

3.3-2 设 f 是环 A 到 A' 的同态,$a\in A, b=f(a)$,则 $f^{-1}(b)=a+\ker f$.

分析 $f^{-1}(b)$是元素 b 的全原像,是个集合,所以通常采用互相包含的证明方法.

证 采用互相包含的证法.

由于 $f(a+\ker f)=f(a)+0'=b$,所以 $a+\ker f\subseteq f^{-1}(b)$.

反之,对任何 $x\in f^{-1}(b), f(x)=b=f(a)$,得 $f(x-a)=0'$,所以 $x-a\in\ker f$ 即 $x\in a+\ker f$. 因而 $f^{-1}(b)\subseteq a+\ker f$.

综上,得 $f^{-1}(b)=a+\ker f$.

3.3-3 证明主教材定理 3.3.1 至定理 3.3.4.

分析 参考群论里类似的定理的证明,并注意环与群的不同. 这个题非常好,一方面复习了过去的内容,另一方面在过去的基础上有所创新.

定理 3.3.1(同态基本定理) 设 $f: A\to A'$是满同态,$K=\ker f$,则(1)存在同构 σ: $A/K\overset{\sigma}{\cong}A'$,(2)$\varphi(a)=a+K\,(A\to A/K)$(称 φ 为 A 到其商环的**自然同态**),则 $f=\sigma\varphi$.

证 (1) 我们可以利用群论的同态基本定理的结果:$\sigma: a+K\mapsto f(a)$是加群$(A,+)/K\cong(A',+)$的同构映射,只需检验对乘法也保持运算:

$$\sigma((a+K)(b+K))=\sigma(ab+K)=f(ab)=f(a)f(b)=\sigma(a)\sigma(b).$$

所以 $\sigma: a+K\mapsto f(a)$是环的同构:$(A,+,\cdot)/K\cong(A',+,\cdot)$.

(2) 设 $\varphi(a)=a+K\,(A\to A/K)$,由群论的定理,对加法保持运算,只需检验对乘法也保持运算:

$$\varphi(ab)=ab+K=(a+K)(b+K)=\varphi(a)\varphi(b),$$

所以 φ 是同态. 又由于

$$\sigma\varphi(a)=\sigma(a+K)=f(a),\quad\forall a\in A,$$

所以 $f=\sigma\varphi$.

定理 3.3.2(子环对应定理) 设 $A\overset{f}{\sim}A', K=\ker f, S=\{H\mid K\leqslant H\leqslant A\}$,

$T=\{N \mid N\leqslant A'\}$，则存在双射 $\tau: H\mapsto f(H)(S\to T)$.

证　根据群论中的子群对应定理，τ 把 $(A,+)$ 中的子群 H 对应 $(A',+)$ 中的子群 $f(H)$，且是一一对应的．现在只要证明当 H 对乘积封闭时，$f(H)$ 也对乘积封闭，反之亦然．即 $a,b\in H\Rightarrow ab\in H$，显然有 $f(a),f(b)\in f(H)\Rightarrow f(a)f(b)=f(ab)\in f(H)$，所以有 H 是子环时，$f(H)$ 也是子环．

反之，对任意一个 $H'\leqslant T$，取 $H=f^{-1}(H')$，则 $H\geqslant K, f(H)=H'$. $\forall a,b\in H$ 有 $f(ab)\in H'$，所以 $ab\in H$，因而 H 是子环．

这就证明了 τ 是 S 到 T 的一个双射．

类似可证 τ 也是理想之间的一个双射．

定理 3.3.3（商环同构定理）　设 $A\overset{f}{\sim}A'$，$K=\ker f$，$K\leqslant I\lhd A$，则 $f(I)\lhd A'$，且

$$A/I\cong A'/f(I)\cong \frac{A/K}{I/K}.$$

证　由于商环是加群的商群，所以直接利用群论的结果得到

$$(A,+)/I\cong (A',+)/f(I).$$

设 $(A,+)/I=\{a+I \mid a\in A\}$，$(A',+)/f(I)=\{f(a)+f(I) \mid f(a)\in A'\}$，设 σ: $a+I\mapsto f(a)+f(I)$ 是对应的同构映射，只需再证明 σ 保持乘法运算：

$$\begin{aligned}\sigma((a+I)(b+I)) &=\sigma(ab+I)=f(ab)+f(I)=f(a)f(b)+f(I)\\ &=(f(a)+f(I))(f(b)+f(I))\\ &=\sigma(a+I)\sigma(b+I).\end{aligned}$$

所以两个商环同构．又由于同态基本定理有 $A/K\cong A'$，$I/K\cong f(I)$，因而

$$A/I\cong A'/f(I)\cong \frac{A/K}{I/K}.$$

定理 3.3.4（第二同构定理）　$I\lhd A, H\leqslant A$，则

$$(H+I)/I\cong H/(H\cap I).$$

证　由群论的第二同构定理，对加群此式成立．只需此同构对乘法也保持运算即可．

设 $J=H\cap I$，$\sigma: h+I\mapsto h+J\ ((H+I)/I\to H/(H\cap I))$ 是同构映射，

$$\begin{aligned}\sigma((h_1+I)(h_2+I)) &=\sigma(h_1h_2+I)=h_1h_2+J=(h_1+J)(h_2+J)\\ &=\sigma((h_1+I))\sigma((h_2+I)).\end{aligned}$$

所以等式成立．

点评　上述证明都利用了群论的相应结果，也可以参考群论中的证明方法重新证明，读者不妨自己按此做一下．

3.3-4　利用同态基本定理证明

(1) $\mathbb{R}[x]/(x^2+1)\equiv(\mathbb{C},+,\cdot)$;

(2) $F[x]/(x)\equiv(F,+,\cdot)$, F 为数域.

分析 利用同态基本定理证明 $A/I\cong A'$ 的方法为：第一步是找一个 A 到 A' 的满同态，第二步是求此同态的核正好是 I，则问题就解决了.

证 (1)作映射 $\varphi: f(x)\mapsto f(\mathrm{i})(\mathbb{R}[x]\to C)$,

由于 $\forall f(x),g(x)\in\mathbb{R}[x]$，有

$$\varphi(f(x)+g(x)) = f(\mathrm{i})+g(\mathrm{i}) = \varphi(f(x))+\varphi(g(x)),$$
$$\varphi(f(x)g(x)) = f(\mathrm{i})g(\mathrm{i}) = \varphi(f(x))\varphi(g(x)),$$

故 φ 是同态. 易证它是满同态：$\forall a+b\mathrm{i}\in\mathbb{C}$，取 $f(x)=a+bx$，则 $\varphi(f(x))=a+b\mathrm{i}$.

下面求同态核：

$$\begin{aligned}\ker\varphi &=\{f(x)\in\mathbb{R}[x]\mid f(\mathrm{i})=0\}\\ &=\{f(x)\in\mathbb{R}[x]\mid (x-\mathrm{i})\mid f(x)\}\\ &=\{f(x)\in\mathbb{R}[x]\mid (x^2+1)\mid f(x)\}\\ &=(x^2+1).\end{aligned}$$

所以由同态基本定理得

$$\mathbb{R}[x]/(x^2+1)\equiv(\mathbb{C},+,\cdot).$$

(2) 作映射 $\varphi: f(x)\mapsto f(0)(F[x]\to F)$,

由于 $\forall f(x),g(x)\in\mathbb{R}[x]$，有

$$\varphi(f(x)+g(x)) = f(0)+g(0) = \varphi(f(x))+\varphi(g(x)),$$
$$\varphi(f(x)g(x)) = f(0)g(0) = \varphi(f(x))\varphi(g(x)),$$

故 φ 是同态. 易证它是满同态：$\forall a\in F$，取 $f(x)=a+x$，则 $\varphi(f(x))=a$.

下面求同态核：

$$\begin{aligned}\ker\varphi &=\{f(x)\in F[x]\mid f(0)=0\}\\ &=\{f(x)\in F[x]\mid x\mid f(x)\}\\ &=(x).\end{aligned}$$

所以由同态基本定理得

$$F[x]/(x)\equiv(F,+,\cdot).$$

3.3-5 将复数环同构嵌入 $(M_2(\mathbb{R}),+,\cdot)$ 中.

分析 首先写出这两个环的元素，所谓“同构嵌入”指寻找一个单同态. 找的方法是首先确定一些特殊元素的像，例如单位元、生成元等，然后找出一般的映射，并证明它是同态.

解 写出这两个环的元素：

$$C=\{a+b\mathrm{i}\mid a,b\in\mathbb{R}\},\quad M_2(\mathbb{R})=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}\mid a,b,c,d\in\mathbb{R}\right\}.$$

设 f 是 C 到 $M_2(\mathbb{R})$ 的一个单同态,则应把单位元映成单位元,即

$$f(1)=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}.$$

因 i 是 C 中的一个乘法 4 阶元,应映成 $M_2(\mathbb{R})$ 中的一个 4 阶元,因而可设(当然要经过试验)

$$f(\mathrm{i})=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}.$$

于是得到

$$f(a+b\mathrm{i})=\begin{bmatrix}a & b\\ -b & a\end{bmatrix},\quad \forall a+b\mathrm{i}\in\mathbb{C}.$$

我们来证明它保持运算(其实可以不必证明,但为了放心,还是证一下):

$$f(a+b\mathrm{i}+c+d\mathrm{i})=f(a+c+(b+d)\mathrm{i})=\begin{bmatrix}a+c & b+d\\ -(b+d) & a+c\end{bmatrix}$$
$$=\begin{bmatrix}a & b\\ -b & a\end{bmatrix}+\begin{bmatrix}c & d\\ -d & c\end{bmatrix}=f(a+b\mathrm{i})+f(c+d\mathrm{i}),$$
$$f((a+b\mathrm{i})(c+d\mathrm{i}))=f(ac-bd+(ad+bc)\mathrm{i})$$
$$=\begin{bmatrix}ac-bd & ad+bc\\ -(ad+bc) & ac-bd\end{bmatrix}$$
$$=\begin{bmatrix}a & b\\ -b & a\end{bmatrix}\begin{bmatrix}c & d\\ -d & c\end{bmatrix}$$
$$=f(a+b\mathrm{i})f(c+d\mathrm{i}).$$

所以 f 是同态映射,显然是单同态(确实很显然).

所以 f 把复数环同构嵌入 $(M_2(\mathbb{R}),+,\cdot)$ 中.

点评　是否可找到其他的单同态?

3.3-6　找出 $(Z_n,+,\cdot)$ 上一切自同态.

分析　与前面的题类似,解决这类问题通常是根据同态定义找出一些特殊元素,例如单位元,生成元等的像,再找出一般元素的像,从而确定所有同态映射.

解　方法类似于本节例 3.3.4.

设 $Z_n=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$,设 f 是 $(Z_n,+,\cdot)$ 上任一自同态,可设 $f(\bar{1})=\bar{k}$,则

由保持加法运算，得对任意 $\bar{x}\in Z_n$ 有 $f(\bar{x})=\overline{kx}$.

由保持乘法运算，$f(\bar{x}\cdot\bar{y})=\overline{kxy}=f(\bar{x})f(\bar{y})=\overline{k^2xy}$，如果 $\bar{x}\cdot\bar{y}=\bar{0}$，对任意 k 都成立；如果 $\bar{x}\cdot\bar{y}\neq\bar{0}$ 得，方程 $\bar{k}=\bar{k}^2$，即 $\bar{k}(\bar{k}-\bar{1})=\bar{0}$，有解：$\bar{k}=\bar{0}$，$\bar{k}=\bar{1}$，但还可能有其他的解，例如，在$(Z_6,+,\cdot)$中方程 $\bar{k}(\bar{k}-\bar{1})=\bar{0}$，有解：$\bar{k}=\bar{0}$，$\bar{k}=\bar{1}$，$\bar{k}=\bar{3}$，$\bar{k}=\bar{4}$. 所以一般来说，都有以下两个自同态：

对 $\bar{k}=\bar{0}$，对应的是零同态：$f_0(\bar{x})=\bar{0}$，$\forall\bar{x}\in Z_n$.

对 $\bar{k}=\bar{1}$，对应的是单位同态：$f_1(\bar{x})=\bar{x}$，$\forall\bar{x}\in Z_n$.

对具体的 n 还可能有其他的自同态.

所以

$$\mathrm{End}(Z_n,+,\cdot)=\{f_0,f_1,\cdots\}.$$

当 $n=p$（素数）时，$\mathrm{End}(Z_p,+,\cdot)=\{f_0,f_1\}$.

点评 对比一下群$(Z_n,+)$的自同态半群 $\mathrm{End}(Z_n,+)$. 由于环的运算有两种，大大限制了自同态的存在.

3.3-7 $A=\{(a_1,a_2,\cdots,a_n)\mid a_i\in\mathbb{Z}\}$对向量的加法构成群，$E(A)$为 A 上的自同态环，证明$(E(A),+,\cdot)\cong(M_n(\mathbb{Z}),+,\cdot)$.

分析 先看懂题目，A 是全体整数分量的 n 维向量的集合，显然，对向量的加法构成群. $M_n(\mathbb{Z})$是全体整数分量的 n 阶矩阵的集合.

证 首先要确定 $E(A)$.

设 f 为 A 上的任一自同态. 由于

对任意 $\alpha,\beta\in A$ 有 $f(\alpha+\beta)=f(\alpha)+f(\beta)$，

对任意 $k\in\mathbb{Z}$ 有 $f(k\alpha)=kf(\alpha)$.

所以 f 是 A 上的线性变换，用线性代数的方法可得

$$f(\alpha)=B\alpha,\quad B\in M_n(\mathbb{Z}).$$

反之，对任意 $B\in M_n(\mathbb{Z})$，定义 A 上的变换 f_B 为

$$f_B(\alpha)=B\alpha.$$

则不难证明 f_B 是 A 上的一个自同态.

下证$(E(A),+,\cdot)\cong(M_n(\mathbb{Z}),+,\cdot)$：

作映射 $\sigma: f_B\mapsto B(E(A)\to M_n(\mathbb{Z}))$.

由加群的自同态环的定义（请查阅 3.1 节内容提要或主教材上相关内容），$\forall f_B,f_c\in E(A)$有

$$(f_B+f_c)(\alpha)=f_B(\alpha)+f_c(\alpha)=B\alpha+C\alpha=(B+C)\alpha,$$

$$(f_Bf_c)(\alpha)=f_B(f_c(\alpha))=BC\alpha.$$

因而

$$\sigma(f_B+f_c)=B+C=\sigma(f_B)+\sigma(f_c),$$
$$\sigma(f_Bf_c)=BC=\sigma(f_B)\sigma(f_c).$$

故 σ 是同态.易见 σ 是满同态,不难证明 σ 也是单射,因而 σ 是同构.

所以 $(E(A),+,\cdot)\cong(M_n(\mathbb{Z}),+,\cdot)$.

点评　此题证明过程比较长,注意保持清醒头脑,把每一步表达清楚.其中用到线性代数中的线性变换,但有一点区别.线性代数中的线性变换对应矩阵的元素是在数域里,而本题矩阵的元素是在整数环里.

3.3-8　$m,r\in\mathbb{Z}^+$, $r|m$, $Z_m=\{\bar{0},\bar{1},\cdots,\overline{m-1}\}$, $Z_r=\{0,1,\cdots,r-1\}$,均为同余类环.证明 $f:\bar{a}\mapsto a$ 是 Z_m 到 Z_r 的同态映射,并求 $\ker f$, $Z_m/(\ker f)$.

分析　遇到两个以上同余类环时,其元素应用不同的记号,以免混淆.

证　首先要验证一下 f 是映射,因为如果对一般的 m,r 这样的 f 不一定是映射.

由于 $\bar{a}=\bar{b}\Rightarrow m|(a-b)\Rightarrow r|(a-b)\Rightarrow a=b(\bmod r)$,故 f 是映射.

再证是同态映射:由于

$$f(\bar{a}+\bar{b})=f(\overline{a+b})=a+b=f(\bar{a})+f(\bar{b}),$$
$$f(\bar{a}\cdot\bar{b})=f(\overline{ab})=ab=f(\bar{a})f(\bar{b}),$$

故 f 是同态,且显然是满同态.

求核:设 $m=rs$,则由核的定义,得

$$\ker f=\{\bar{x}\mid x=0\}=\{\bar{0},\bar{r},\overline{2r},\cdots,\overline{(s-1)r}\}\cong(Z_s,+,\cdot).$$

所以由同态基本定理得

$$(Z_m,+,\cdot)/(\ker f)=\{\bar{h}+\ker f\mid h=0,1,\cdots,r-1\}\cong(Z_r,+,\cdot).$$

点评　此题得到了一个一般的结果:当 $m=rs$ 时,有

$$(Z_m,+,\cdot)/(Z_s,+,\cdot)\cong(Z_r,+,\cdot).$$

***3.3-9**　证明 $\mathrm{Aut}\mathbb{Z}[x]\cong\left\{\begin{bmatrix}1&a\\0&\varepsilon\end{bmatrix}\middle|\varepsilon=\pm1,a\in\mathbb{Z}\right\}$.

分析　首先分析左边的 $\mathrm{Aut}(\mathbb{Z}[x],+,\cdot)$,与前面分析的方法类似,要抓住生成元的可能的像.求出 $\mathrm{Aut}(\mathbb{Z}[x],+,\cdot)$后问题就好办了.

证　由于 $\mathbb{Z}[x]=\langle 1,x\rangle$,设 σ 为 $\mathbb{Z}[x]$ 上任一自同构,则必有 $\sigma(1)=1$, $\sigma(x)=\varepsilon x+a$, $\varepsilon=\pm1$, $a\in\mathbb{Z}$.这是因为要保证 σ 是满射,其他情况都不是满射.

令

$$\sigma_{\varepsilon,b}(f(x))=f(\varepsilon x+a),\quad\forall f(x)\in\mathbb{Z}[x].$$

易证 $\sigma_{\varepsilon,b}$ 是 $\mathbb{Z}[x]$ 上的满射,并保持运算(确实很容易,留给读者自己做).故得

$\mathrm{Aut}\mathbb{Z}[x]=\{\sigma_{\varepsilon,a}\mid\varepsilon=\pm1,\quad a\in\mathbb{Z},\quad\sigma_{\varepsilon,a}(f(x))=f(\varepsilon x+a)\}.$

下面证明它与右边的矩阵群同构：作映射

$$\varphi:\sigma_{\varepsilon,a}\mapsto\begin{bmatrix}1&a\\0&\varepsilon\end{bmatrix},$$

显然是双射，下面证明保持运算.

我们先看群 $\mathrm{Aut}\mathbb{Z}[x]$中元素的乘法：

$$\sigma_{\varepsilon,a}\sigma_{\eta,c}(f(x))=\sigma_{\varepsilon,a}(f(\eta x+c)=f(\varepsilon\eta x+\eta a+c)=\sigma_{\varepsilon\eta,\eta a+c}.$$

因而

$$\begin{aligned}\varphi(\sigma_{\varepsilon,a}\sigma_{\eta,c})&=\varphi(\sigma_{\varepsilon\eta,\eta a+c})=\begin{bmatrix}1&\eta a+c\\0&\varepsilon\eta\end{bmatrix}=\begin{bmatrix}1&a\\0&\varepsilon\end{bmatrix}\begin{bmatrix}1&c\\0&\eta\end{bmatrix}\\&=\varphi(\sigma_{\varepsilon,a})\varphi(\sigma_{\eta,c}),\end{aligned}$$

所以

$$\mathrm{Aut}\mathbb{Z}[x]\cong\left\{\begin{bmatrix}1&a\\0&\varepsilon\end{bmatrix}\middle|\varepsilon=\pm1,a\in\mathbb{Z}\right\}.$$

点评 该题涉及概念很多，计算也比较复杂，必须耐心完成.

3.3-10 求$\mathbb{Z}[i]$、$\mathbb{Z}[x]$和偶数环的分式域.

分析 分式域就是在整环中对所有元素作可能的分式所得到的集合.

解 (1)由分式域的定义，可得

$$\begin{aligned}P(\mathbb{Z}[\mathrm{i}])&=\left\{\frac{a+b\mathrm{i}}{c+d\mathrm{i}}\middle|a,b,c,d\in\mathbb{Z},cd\neq0\right\}\\&=\left\{\frac{ac+bd+(bc-ad)\mathrm{i}}{c^2+d^2}\middle|a,b,c,d\in\mathbb{Z},cd\neq0\right\}\\&=\{\alpha+\beta\mathrm{i}\mid\alpha,\beta\in\mathbb{Q}\}=\mathbb{Q}[\mathrm{i}].\end{aligned}$$

(2) $P(\mathbb{Z}[x])=\left\{\dfrac{f(x)}{g(x)}\middle|f(x),g(x)\in\mathbb{Z}[x],g(x)\neq0\right\}$,

由于$\mathbb{Q}\subset P(\mathbb{Z}[x])$，因而也可表示为

$$P(\mathbb{Z}[x])=\left\{\frac{f(x)}{g(x)}\middle|f(x),g(x)\in\mathbb{Q}[x],g(x)\neq0\right\}.$$

(3) 设偶数环为

$$A=\{2n\mid n\in\mathbb{Z}\},$$

则

$$P(A)=\left\{\frac{2p}{2q}\middle|p,q\in\mathbb{Z},q\neq0\right\}=\left\{\frac{p}{q}\middle|p,q\in\mathbb{Z},q\neq0\right\}=\mathbb{Q}.$$

点评 该题主要熟悉一下分式域的概念.

3.4 整环中的因子分解

一、内容提要

我们熟悉整数运算中的一大问题就是研究整数中的素数的性质、整数的因子分解以及求两(多)个整数的最大公因子、最小公倍数等问题. 现在我们要把这些问题推广到整环中去,这一节和后面几节做的都是这一推广工作. 我们研究的对象是有单位元的整环.

设 D 是有单位元的整环,$U(D)$是 D 中的可逆元集合.

1. 一些基本概念

设 $a,b,c,d\in D$.

- **因子**: 若 $c=ab$,则称 a 是 c 的因子,c 是 a 的倍元,并记作 $a|c$(称为 a 整除 c). 若 a 与 b 都不是可逆元,则称 a 是 c 的真因子. 可逆元无真因子,因而在除环和域内无因子分解问题.
- **相伴**: $a\sim b$: $a|b$ 且 $b|a$. $a\sim b\Leftrightarrow \exists\, u\in U(D)$使 $a=ub$.
- **既约元**(不可约元): $p\in D\backslash U(D)$, p 无真因子.
- **素元**: $p\in D\backslash U(D)$满足: $p|ab\Rightarrow p|a$ 或 $p|b$.
- **最大公因子**: 设 $a,b\in D$,若有 $d\in D^*$ 满足(1)$d|a$ 且 $d|b$,(2)如果有 d'满足 $d'|a$ 且 $d'|b$,则 $d'|d$. 则称 d 是 a 与 b 的最大公因子,记作 $d\sim(a,b)$.(由于在一般整环里最大公因子不惟一,但互相相伴,所以用相伴记号. 但在特殊的环里,例如在$\mathbb{Z}$中规定正的最大公因子记作(a,b),是惟一确定的. 另外,在一般整环里,不一定任何两个元素都存在最大公因子,例如在$(\mathbb{Z}(\sqrt{-5}),+,\cdot)$中元素 9 与 $3(2+\sqrt{-5})$就不存在最大公因子.)

类似方法可定义**最小公倍元**.

- **互素**: $(a,b)\sim 1$,称 a 与 b 互素.

2. 若干性质

- p 是素元$\Rightarrow p$ 是既约元.

  一般来说,逆定理不成立. 反例: $(\mathbb{Z}(\sqrt{-5},+,\cdot))$中元素 3 是既约元但不是素元.
- 若 D 中任何两个元素均有最大公因子,则每一个既约元也是素元.
- $((a,b),c)\sim(a,(b,c))$, $(ac,bc)\sim c(a,b)$.

- $(a,b)\sim 1,(a,c)\sim 1\Rightarrow(a,bc)\sim 1$.

既约元与素元是本节的重点.

二、习题 3.4 详细解答

3.4-1 证明相伴关系是等价关系,并满足:$a\sim b,c\sim d\Rightarrow ac\sim bd$.

分析 证明是常规的.

证 先证相伴关系是等价关系:

反身性:因 $a|a$,故 $a\sim a$;

对称性:$a\sim b\Rightarrow a|b,b|a\Rightarrow b\sim a$;

传递性:$a\sim b$ 且 $b\sim c\Rightarrow a|b,b|a;b|c,c|b\Rightarrow a|c,c|a\Rightarrow a\sim c$.

再证对乘法保持运算:

$$a\sim b,\quad c\sim d\Rightarrow a\mid b,\quad b\mid a;\quad c\mid d,$$
$$d\mid c\Rightarrow ac\mid bd,\quad bd\mid ac\Rightarrow ac\sim bd.$$

点评 本题是熟悉一下相伴的概念.

3.4-2 叙述两个元素的最小公倍元的定义,并将最大公因子与最小公倍元的定义推广到多个元素的情形.

分析 复习最大公因子的定义,模仿最大公因子的定义,给出最小公倍元的定义.

答 由最大公因子的定义,类似可得最小公倍元的定义如下:

设 $a,b\in D^*$,若有 $m\in D$ 满足:(1)$a|m$ 且 $b|m$,(2)若有 m'满足,$a|m'$且 $b|m'$,则 $m|m'$. 则称 m 为 a 与 b 的最小公倍元,记作 $m\sim[a,b]$.(由于最小公倍元不惟一,但互相相伴,所以用相伴记号. 但在特殊的环里,例如在$\mathbb{Z}$中规定正的最小公倍元记作$[a,b]$.)

点评 还可进一步推广到多个元素的情形:

定义 设 $a_1,a_2,\cdots,a_k\in D$,若有 $d\in D^*$ 满足:(1)$d|a_1,\cdots,d|a_k$,(2)若有 d'满足 $d'|a_1,\cdots,d'|a_k$,则 $d'|d$. 则称 d 是 a 与 b 的最大公因子,记作 $d\sim(a_1,\cdots,a_k)$.

若有 $m\in D$ 满足:(1)$a_1|m,\cdots,a_k|m$,(2)若有 m'也满足 $a_1|m',\cdots,a_k|m'$,则 $m|m'$. 则记作 $m\sim[a_1,\cdots,a_k]$.

3.4-3 设 D 是有单位的整环,p 为既约元,则(p)为 D 的非平凡理想.

分析 复习既约元的概念.

证 要证$(p)\neq(0)$和$(p)\neq D$.

因为 $p\neq 0$,故$(p)\neq(0)$.

再证$(p)\neq D$. 反证法:假设$(p)=D$,则存在 $q\in D$ 使 $pq=1$,因而 p 是可

逆元，这与 p 是既约元矛盾.

点评　注意我们是在有单位元1的整环中讨论问题，要利用有单位元的条件.

3.4-4　在环 $(\mathbb{Z}[\sqrt{-5}],+,\cdot)$ 中下列元素哪些是既约元？$2,7,29,2-\sqrt{-5},6+\sqrt{-5}$.

分析　复习既约元的概念. 可以逐个用待定系数法检验每个元素是否是既约元. 我们下面先给出判断 $(\mathbb{Z}[\sqrt{-5}],+,\cdot)$ 中一个元素是否是既约元的条件. 先定义 $v(a+b\sqrt{-5})=a^2+5b^2$.

解　我们先证明环 $(\mathbb{Z}[\sqrt{-5}],+,\cdot)$ 中的两个定理：

- **定理1**　设 p 为素数，则 p 是既约元的充分必要条件是 $p\neq a^2+5b^2$，$\forall a,b\in\mathbb{Z}$.

证　首先我们知道 $U(D)=\{1,-1\}$.

必要性：设 p 是既约元. 反证法：假设 $\exists a,b\in\mathbb{Z}$ 使 $p=a^2+5b^2$，显然 $ab\neq 0$，否则与 p 是素数矛盾. 则

$$p=(a+b\sqrt{-5})(a-b\sqrt{-5}),$$

由于 $v(a+b\sqrt{-5})=v(a-b\sqrt{-5})=a^2+5b^2\neq 1$，故 $(a+b\sqrt{-5}),(a-b\sqrt{-5})\notin U(D)$，与 p 是既约元矛盾. 所以 $p\neq a^2+5b^2$，$\forall a,b\in\mathbb{Z}$.

充分性：设 $p\neq a^2+5b^2$，$\forall a,b\in\mathbb{Z}$，要证 p 是既约元.

用反证法：假设 p 不是既约元，则 $p=\alpha\beta$，且 $\alpha,\beta\notin U(D)$，因而 $v(\alpha)\neq 1$，$v(\beta)\neq 1$. 因为 $p^2=v(\alpha)v(\beta)$，故得 $p=v(\alpha)=v(\beta)=a^2+5b^2$，与 $p\neq a^2+5b^2$，$\forall a,b\in\mathbb{Z}$ 矛盾. 所以 p 是既约元.

- **定理2**　设 $\alpha=a+b\sqrt{-5}$，$ab\neq 0$ 且 $(a,b)=1$，则当 $v(\alpha)=a^2+5b^2=p$（素数）或 $ab\neq 0$，$(a,b)=1$ 且 $v(\alpha)<36$ 时，α 是既约元.

证　我们把 $\alpha=a+b\sqrt{-5}$，$ab\neq 0$ 的元素称为真复数.

用反证法：假设 α 不是既约元，则 α 可表示为 $\alpha=\beta\gamma$，$\beta,\gamma\notin U(D)$，因而得到 $v(\alpha)=v(\beta)v(\gamma)$，$v(\beta)>1$，$v(\gamma)>1$. 与 $v(\alpha)$ 是素数矛盾.

由于当 $ab\neq 0$ 时，$v(a+b\sqrt{-5})=a^2+5b^2\geqslant 6$，即真复数的范数大于等于6. 如果 α 不是既约元，则 α 可表示为 $\alpha=\beta\gamma$，$\beta,\gamma\notin U(D)$. 由于 $(a,b)=1$，知 β,γ 是真复数，因而 $v(\beta)\geqslant 6$，$v(\gamma)\geqslant 6$，故 $v(\alpha)\geqslant 36$. 所以当 $ab\neq 0$，$(a,b)=1$ 且 $v(a+b\sqrt{-5})<36$ 时，$\alpha=a+b\sqrt{-5}$ 是既约元.

解　根据定理1，2，7是既约元，29不是，$29=3^2+5\times 2^2=(2+\sqrt{-5})\cdot(2-\sqrt{-5})$.

根据定理 2,$v(2-\sqrt{-5})=9$ 不是素数,但小于 36,所以 $2-\sqrt{-5}$是既约元. $v(6+\sqrt{-5})=41$ 是素数,所以 $6+\sqrt{-5}$是既约元.

点评　这个题比较复杂.

3.4-5　设 D 为有单位元的整环,则 p 是素元的充分必要条件是 $D/(p)$ 是整环.

分析　复习素元的定义.

证　必要性:已知 p 是素元,要证 $D/(p)$是整环,一是要证 $D/(p)\neq 0$;二是要证 $D/(p)$中无零因子.

由本节习题 3.4-3,(p)为非平凡理想,故 $D/(p)\neq 0$.

对任何 $\bar{a},\bar{b}\in D/(p)$,若 $\bar{a}\bar{b}=\bar{0}$,则 $ab\in(p)$,可设 $ab=pq$,故 $p|ab$. 由于 p 是素元,必有 $p|a$ 或 $p|b$,故有 $\bar{a}=\bar{0}$ 或 $\bar{b}=\bar{0}$. 这就证明了 $D/(p)$中无零因子.

所以 $D/(p)$是整环.

充分性:已知 $D/(p)$是整环,要证 p 是素元.

设 $p|ab$,则 $\bar{a}\bar{b}=\bar{0}$,由于 $D/(p)$是整环,必有 $\bar{a}=\bar{0}$ 或 $\bar{b}=\bar{0}$,可得 $p|a$ 或 $p|b$. 所以 p 是素元.

点评　本题一方面是按概念来证明,另一方面,可利用前面习题中的结果.

3.4-6　$\alpha=a+bi\in\mathbb{Z}[i]$,且 $v(\alpha)=a^2+b^2=$素数,证明 α 是$(\mathbb{Z}[i],+,\cdot)$中的既约元.

分析　从既约元的定义出发.

证　设 $\alpha=\beta\gamma$,则 $v(\alpha)=v(\beta)v(\gamma)$,由于 $v(\alpha)=a^2+b^2=$素数,必有 $v(\beta)=1$ 或 $v(\gamma)=1$,即 $\beta\in U(\mathbb{Z}[i])$或 $\gamma\in U(\mathbb{Z}[i])$. 所以 α 是$(\mathbb{Z}[i],+,\cdot)$中的既约元.

点评　本题比较容易.

3.5　惟一分解整环

一、内容提要

本节讨论三类重要的整环,它们互相有紧密的联系,并且应用比较广泛.

设 D 是有单位元的整环,$U(D)$是 D 中的可逆元集合,$U(D)^*=U(D)\backslash\{0\}$.

1. 惟一分解整环

$D^*\backslash U(D)$中任何一个元素可分解为有限个既约元之积,且除次序和相差

可逆元因子外形式是惟一的：

$$a = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_s^{\varepsilon_s}.$$

- D 是惟一分解整环的条件：在 $D^* \setminus U(D)$ 中任何一个元素可分解为有限个既约元之积的条件下有
  D 是惟一分解整环 $\Leftrightarrow D$ 中任何两个元素有最大公因子 $\Leftrightarrow D$ 中的既约元都是素元.
- 重要的例：在 $\mathbb{Z}[\sqrt{-5}]$ 中 $9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5})$，$3,2\pm\sqrt{-5}$ 都是既约元，所以 $\mathbb{Z}[\sqrt{-5}]$ 不是惟一分解环. 3 是既约元，但不是素元. 9 与 $3(2+\sqrt{-5})$ 没有最大公因子.

2. 主理想整环

每一个理想都是主理想（由一个元素生成的理想）的整环.

- 重要的例：整数环 $(\mathbb{Z},+,\cdot)$，域上多项式环 $(F[x],+,\cdot)$ 都是主理想整环. 但 $(\mathbb{Z}[x],+,\cdot)$ 不是主理想整环.
- 主理想整环的性质：主理想整环是惟一分解整环. 在主理想整环中最大公因子定理成立. 设 D 是主理想整环，p 是既约元，则 $D/(p)$ 是域.

3. 欧氏整环

可实行带余除法的整环. 详细定义如下：若存在映射 $v: D^* \to \mathbb{Z}^+$ 满足：$\forall a\in D^*$，$\forall b\in D$ 均有 $q,r\in D$ 使

$$b = qa + r,$$

其中 $r=0$ 或 $v(r)<v(a)$，则称 D 是一个欧氏整环，$v(a)$ 称为 a 的范数.

- 整数环 $(\mathbb{Z},+,\cdot)$，可定义 $v(x)=|x|$，因而是欧氏整环. 注意与整数的带余除法略有区别，原因是映射 v 对 0 没有定义，因而要单独列出 $r=0$ 的情况.
- 域上多项式环 $(F[x],+,\cdot)$，可定义 $v(f(x))=\deg f(x)+1$，因而是欧氏整环. 也可定义 $v(f(x))=2^{\deg f(x)}$，这时满足：$v(f(x)g(x))=v(f(x))v(g(x))$，有时有用.

用辗转相除法求两个多项式的最大公因式. $F(x)$ 中的不可约元称为不可约多项式. 多项式 $f(x)$ 无重根的充要条件是 $(f(x),f'(x))=1$.

- 高斯整数环 $(Z[\mathrm{i}],+,\cdot)$，可定义 $v(a+b\mathrm{i})=a^2+b^2$，因而是欧氏整环.

4. 一些结果

- 三个整环的关系：

D 是欧氏整环 $\Rightarrow D$ 是主理想整环 $\Rightarrow D$ 是惟一分解整环.

- 在主理想整环里，最大公因子公式 $pa+qb=d$ 成立，且有

  (1) $(a,b)\sim 1 \Leftrightarrow \exists\, p,q\in D: pa+qb=1$.

  (2) $a\mid bc$ 且 $(a,b)\sim 1\Rightarrow a\mid c$.

  (3) 设 p 为既约元(素元)，则有 $p\mid ab\Rightarrow p\mid a$ 或 $p\mid b$.

  (4) $(a,b)\sim 1$ 且 $(a,c)\sim 1\Rightarrow (a,bc)\sim 1$.

  (5) $a\mid c, b\mid c$ 且 $(a,b)\sim 1\Rightarrow ab\mid c$.

  (6) $(a,b)[a,b]\sim ab$.

  因而把整数中有关的性质推广到主理想整环. 特别是在多项式环里应用这些性质.

- 域的乘群的任何有限子群是循环群.

二、习题 3.5 详细解答

3.5-1 利用 3.5 节定理 3.5.2 证明域 F 上的多项式环 $F[x]$ 是惟一分解整环.

分析 复习该定理. 要证以下两点：(1)证明 $F[x]$ 中任一真因子序列含有限项. $F[x]$ 中任意两个非零多项式都有最大公因子.

证 (1) 证明 $F[x]$ 中任一真因子序列含有限项.

设 $f(x)$ 为 $F[x]$ 中 $\deg f(x)=n>0$ 的任一多项式，若 $g(x)$ 是 $f(x)$ 的真因子，则 $\deg g(x)<n$. 由于小于 n 的正整数只有有限个，所以，$f(x)$ 的多项式真因子序列也只有有限个.

(2) $F[x]$ 中任意两个非零多项式都有最大公因子. 在高等代数中我们单独证明了数域上任意两个非零多项式都有最大公因子.

综上，$F[x]$ 是惟一分解整环.

3.5-2 证明 $\mathbb{Z}[\sqrt{-5}]$ 满足定理 3.5.2 条件 Ⅰ.

分析 对照定理 3.5.2 条件 Ⅰ.

证 定理 3.5.2 条件 Ⅰ：任一元素的真因子序列含有限项.

任取一个非 0 元素 $\alpha=a+b\sqrt{-5}$，则 $v(\alpha)=a^2+5b^2\in\mathbb{Z}^+$，设 α_1 是 α 的真因子，则 $v(\alpha_1)<v(\alpha)$. 类似地，若 α_2 是 α_1 的真因子，则 $v(\alpha_2)<v(\alpha_1)$，…. 由于小于 $v(\alpha)$ 的正整数只有有限个，所以，α 的真因子序列含有限项.

3.5-3 证明 $\mathbb{Z}[\sqrt{10}]$ 不是惟一分解整环.

分析 应用定理 3.5.2.

证 利用定理 3.5.2 条件 Ⅱ：任一既约元都是素元.

考虑元素 3，显然是既约元. 由于 $3\mid(1+\sqrt{10})(1-\sqrt{10})$，但 3 不能整除 $(1+\sqrt{10})$，也不能整除 $(1-\sqrt{10})$. 故 3 不是素元，所以 $Z[\sqrt{10}]$ 不是惟一分解整环.

3.5-4 证明在惟一分解整环中有 $ab\sim(a,b)[a,b]$.

分析 利用元素的分解式.

证 由于 a 和 b 可分解为既约元的乘积，且形式是惟一的. 因而可将它们表示为

$$a = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}, \quad r_i \geqslant 0$$

$$b = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}, \quad t_i \geqslant 0.$$

其中 $p_1, p_2, \cdots, p_s$ 是不同的既约元. r_i 与 t_i 不同时为 0. 令

$$m_i = \min(r_i, t_i), \quad n_i = \max(r_i, t_i), \quad i = 1, 2, \cdots, s.$$

则得到

$$(a,b) \sim p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}, \quad [a,b] \sim p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s},$$

并有

$$m_i + n_i = r_i + s_i, \quad i = 1, 2, \cdots, s.$$

所以 $ab\sim(a,b)[a,b]$.

点评 证明方法与整数中相应的公式是相同的.

3.5-5 下列环是否是欧氏整环? 并证明之.

(1) $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$;

(2) $\mathbb{Z}[\sqrt{-2}]=\{a+b\sqrt{-2}\mid a,b\in\mathbb{Z}\}$;

(3) $\mathbb{Z}[\sqrt{-3}]=\{a+b\sqrt{-3}\mid a,b\in\mathbb{Z}\}$;

(4) $\mathbb{Z}[\sqrt{-3}]=\left\{a+b\sqrt{-3}\,\middle|\, a,b\in\mathbb{Z}\text{ 且 }a,b\text{ 同为整数,或同为奇数的}\frac{1}{2}\right\}$.

分析 复习欧氏整环的概念与证明方法. 要证明一个整环 D 是欧氏整环，关键是找到一个映射 $v: D^* \to \mathbb{Z}^+$，满足带余除法的条件. $v(\alpha)$ 称为 α 的范数，满足 $v(\alpha\beta)=v(\alpha)v(\beta)$.

如果找不到这样的范数，则可猜想 D 不是欧氏整环，要证明 D 不是欧氏整环，只要在 D 中找到一个既约元不是素元，或找到两个元素没有最大公因子.

解与证 (1) $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$.

定义 $v(\alpha)=|a^2-2b^2|$，是 $D^*\to\mathbb{Z}^+$ 的映射，且满足 $v(\alpha\beta)=v(\alpha)v(\beta)$.

$\forall\alpha=a+b\sqrt{2}\neq 0$, $\beta=c+d\sqrt{2}$，令 $q=u+w\sqrt{2}$, $\beta=q\alpha+r$，得

$$r=\alpha\left[\left(\frac{ac-2bd}{a^2-2b^2}-u\right)+\left(\frac{ad-bc}{a^2-2b^2}-w\right)\sqrt{2}\right],$$

可适当选择 u 和 w 使 $\left|\frac{ac-2bd}{a^2-2b^2}-u\right|\leqslant\frac{1}{2}$，$\left|\frac{ad-bc}{a^2-2b^2}-w\right|\leqslant\frac{1}{2}$，则得 $r=0$ 或(注意到 $v(\alpha\beta)=v(\alpha)v(\beta)$ 不仅在 $\mathbb{Z}[i]$ 中成立，而且在整个复数环中都成立.)

$$\begin{aligned}v(r)&=v(\alpha)v\left[\left(\frac{ac-2bd}{a^2-2b^2}-u\right)+\left(\frac{ad-bc}{a^2-2b^2}-w\right)\sqrt{2}\right]\\&\leqslant v(\alpha)\left(\frac{1}{4}+\frac{2}{4}\right)<v(\alpha).\end{aligned}$$

所以($\mathbb{Z}[\sqrt{2}]$，+，·)是欧氏环.

(2) $\mathbb{Z}[\sqrt{-2}]=\{a+b\sqrt{-2}\mid a,b\in\mathbb{Z}\}$.

方法类似(1).

定义 $v(\alpha)=a^2+2b^2$，是 $D^*\to Z^+$ 的映射，且满足 $v(\alpha\beta)=v(\alpha)v(\beta)$.

$\forall\alpha=a+b\sqrt{-2}\neq0,\beta=c+d\sqrt{-2}$，令 $q=u+w\sqrt{-2},\beta=q\alpha+r$，得

$$r=\alpha\left[\left(\frac{ac+2bd}{a^2+2b^2}-u\right)+\left(\frac{ad-bc}{a^2+2b^2}-w\right)\sqrt{-2}\right],$$

可适当选择 u 和 w 使 $\left|\frac{ac+2bd}{a^2+2b^2}-u\right|\leqslant\frac{1}{2}$，$\left|\frac{ad-bc}{a^2+2b^2}-w\right|\leqslant\frac{1}{2}$，则得 $r=0$ 或

$$\begin{aligned}v(r)&=v(\alpha)v\left[\left(\frac{ac-2bd}{a^2+2b^2}-u\right)+\left(\frac{ad-bc}{a^2+2b^2}-w\right)\sqrt{-2}\right]\\&\leqslant v(\alpha)\left(\frac{1}{4}+\frac{2}{4}\right)<v(\alpha).\end{aligned}$$

所以($\mathbb{Z}[\sqrt{-2}]$，+，·)是欧氏环.

(3) $\mathbb{Z}[\sqrt{-3}]=\{a+b\sqrt{-3}\mid a,b\in\mathbb{Z}\}$.

用类似的方法定义 $v(\alpha)=a^2+3b^2$，最后得到

$$\begin{aligned}v(r)&=v(\alpha)v\left[\left(\frac{ac-3bd}{a^2+3b^2}-u\right)+\left(\frac{ad-bc}{a^2+3b^2}-w\right)\sqrt{-3}\right]\\&\leqslant v(\alpha)\left(\frac{1}{4}+\frac{3}{4}\right)=v(\alpha).\end{aligned}$$

不是严格的小于. 所以我们怀疑它不是欧氏整环.

由于 $4=(1+\sqrt{-3})(1-\sqrt{-3})$，元素 2 显然是既约元，$2\mid(1+\sqrt{-3})\cdot(1-\sqrt{-3})$，但 $2\nmid(1+\sqrt{-3})$ 和 $2\nmid(1-\sqrt{-3})$，所以 2 不是素元，从而($\mathbb{Z}[\sqrt{-2}]$，+，·)不是欧氏整环.

(4) $D=\left\{a+b\sqrt{-3}\,\middle|\,a,b\in\mathbb{Z}\text{ 且 }a,b\text{ 同为整数,或同为奇数的}\frac{1}{2}\right\}$.

用类似的方法定义 $v(\alpha)=a^2+3b^2$,最后得到

$$v(r)=v(\alpha)v\left[\left(\frac{ac-3bd}{a^2+3b^2}-u\right)+\left(\frac{ad-bc}{a^2+3b^2}-w\right)\sqrt{-3}\right]$$

由于 u,w 可取同为整数,或同为奇数的 1/2,可取适当的 u 使 $\left|\frac{ac+3bd}{a^2+3b^2}-u\right|\leqslant\frac{1}{4}$,同时取与 u 同类的数使 $\left|\frac{ad-bc}{a^2+3b^2}-w\right|\leqslant\frac{1}{2}$,因而

$$\begin{aligned}v(r)&=v(\alpha)v\left[\left(\frac{ac-3bd}{a^2+3b^2}-u\right)+\left(\frac{ad-bc}{a^2+3b^2}-w\right)\sqrt{-3}\right]\\&\leqslant v(\alpha)\left(\frac{1}{16}+\frac{3}{4}\right)<v(\alpha).\end{aligned}$$

所以 D 是欧氏环.

点评 这几个题非常典型,要仔细辨别它们的区别.方法上有一致性.当从正面证明时,由带余除法得到 $r=\beta-q\alpha$,然后在复数域里考虑问题:$r=\alpha(\beta\alpha^{-1}-q)$,$v(r)=v(\alpha)v(\beta\alpha^{-1}-q)$,能否选择适当的 q 满足 $v(r)<v(\alpha)$.当不能证明时,是否能举出反例.

3.5-6 p 为奇素数,$a\neq 0(\text{mod } p)$,则 $x^2\equiv a(\text{mod } p)$在$\mathbb{Z}$中有解的充分必要条件是 $a^{\frac{(p-1)}{2}}\equiv 1(\text{mod } p)$.并由此证明当 p 为形如 $4n+1(n\in\mathbb{Z}^+)$的素数时,p 不是$\mathbb{Z}[\mathrm{i}]$中的素元.

分析 这个题涉及概念较多,只能一步一步来.首先要熟悉同余式的意义.

证 先证第一问.

必要性:设 $x^2\equiv a(\text{mod } p)$ 在 $\mathbb{Z}$ 中有解,其解为 $x=b$.则有 $b^2\equiv a(\text{mod } p)$,因而 $a^{\frac{(p-1)}{2}}\equiv b^{p-1}(\text{mod } p)$.由 $a\neq 0(\text{mod } p)$,得 $b\neq 0(\text{mod } p)$.故 $\bar{b}\in Z_p^*$.考虑乘群$(Z_p^*,\cdot)$的阶为 $p-1$,故有 $\bar{b}^{p-1}=\bar{1}$,即 $b^{p-1}\equiv 1(\text{mod } p)$,所以 $a^{\frac{(p-1)}{2}}\equiv 1(\text{mod } p)$.

充分性:设 a 满足 $a^{\frac{(p-1)}{2}}\equiv 1(\text{mod } p)$,要证 $x^2\equiv a(\text{mod } p)$在$\mathbb{Z}$中有解.

考虑多项式 $f(x)=x^{\frac{(p-1)}{2}}-1\in Z_p[x]$,$\bar{a}$ 是 $f(x)$的一个根.可以看出 $\bar{1}^2,\bar{2}^2,\cdots,\left(\overline{\frac{(p-1)}{2}}\right)^2$ 都是 $f(x)$的根.且可证这些根互不相同:

$\bar{a}^2=\bar{b}^2\Rightarrow\bar{a}^2-\bar{b}^2=\bar{0}\Rightarrow p\mid(a-b)(a+b)$,由于 $0<a,b\leqslant\frac{(p-1)}{2}$,故有 $0<a+b\leqslant p-1$,因而$(p,a+b)=1$,得 $p\mid(a-b)$.又由于$|a-b|\leqslant\frac{(p-1)}{2}$,

所以 $a=b$.

这就是说 $\bar{1}^2,\bar{2}^2,\cdots,\left(\overline{\frac{(p-1)}{2}}\right)^2$ 是 $f(x)$的全部根(因为 $Z_p[x]$是惟一分解环,多项式的根的个数等于多项式的次数).因而 $\bar{a}$ 必在其中,即有某个 c 使 $\bar{a}=\bar{c}^2$,即 $c^2\equiv a(\text{mod }p)$,所以方程 $x^2\equiv a(\text{mod }p)$在$\mathbb{Z}$中有解.

第二个问题:证明当 p 为形如 $4n+1(n\in\mathbb{Z}^+)$的素数时,p 不是$\mathbb{Z}[\mathrm{i}]$中的素元.

设 $p=4n+1(n\in\mathbb{Z}^+)$.考虑方程 $x^2\equiv-1(\text{mod }p)$.由于$(-1)^{\frac{(p-1)}{2}}\equiv 1(\text{mod }p)$,由刚证明的结论,方程 $x^2\equiv-1(\text{mod }p)$在$\mathbb{Z}$中有解,设其解为 u,$0<u\leqslant\frac{(p-1)}{2}$,则得 $u^2\equiv-1(\text{mod }p)$,即 $u^2+1\equiv0(\text{mod }p)$.

在环$\mathbb{Z}[\mathrm{i}]$中考虑 $u^2+1\equiv0(\text{mod }p)$,得 $p\mid(u^2+1)\Rightarrow p\mid(u+\mathrm{i})(u+\mathrm{i})$,由于 p 既不能整除 $u+\mathrm{i}$,也不能整除 $u-\mathrm{i}$,所以 p 不是素元.

点评 该题有一定的难度.

3.5-7 设 p 是素数,则 p 是$\mathbb{Z}[\mathrm{i}]$中的素元的充分必要条件是 $p\equiv 3(\text{mod }4)$.

分析 此题与前一题有关.

证 首先 $p=2=(1+\mathrm{i})(1-\mathrm{i})$不是既约元,所以下设 p 是奇素数.

必要性:由习题 3.5-6.

充分性:已知 $p\equiv3(\text{mod }4)$,要证 p 是$\mathbb{Z}[\mathrm{i}]$中的素元.

用反证法:假设 p 不是$\mathbb{Z}[\mathrm{i}]$中的素元,因而也不是既约元,p 有真分解式:$p=\alpha\beta$,其中 α,β都不是可逆元.

设 $v(\alpha)$是 α 的范数,则有 $v(p)=p^2=v(\alpha)v(\beta)$,由于 $v(\alpha),v(\beta)>1$,必有 $v(\alpha)=v(\beta)=p$.令 $\alpha=a+b\mathrm{i}$,得 $p=a^2+b^2$,且 a 与 b 的奇偶性相反(否则 a^2+b^2 不是素数),所以 $p=(2n)^2+(2k+1)^2\equiv1(\text{mod }4)$,矛盾.

点评 由以上的结果,我们大致可知$\mathbb{Z}[\mathrm{i}]$中哪些元素是素元了,详情见本章补充题.

3.6 多项式分解问题

一、内容提要

本节的内容是把高等代数(可能有些同学没有学过,但不影响学习这一节内容)中的整数系数多项式与有理数系数多项式的关系,推广到一般的整环系数多项式与分式域系数多项式的关系.

1. $D[x]$中多项式的性质

设 D 是惟一分解整环，$D[x]$是 D 上的多项式环，则 $U(D[x])=U(D)$.

- 本原多项式的性质：本原多项式指多项式的系数的最大公因子与 1 相伴.

  高斯引理　两个本原多项式之积仍为本原多项式.
- $D[x]$中任何一个非零多项式(通过提出系数的最大公因子)可表示为一个本原多项式与一个非零元之积：

  $\forall f(x)\in D[x]^*$，$f(x)=d\varphi(x)$，其中 $d\in D^*$，$\varphi(x)$是本原多项式.
- D 是惟一分解整环，$D[x]$也是惟一分解整环.
- **多项式的次数**：设 $D[x]$是惟一分解整环，$f(x)\in D[x]$，$f(x)$中 x 的最高次幂称为 $f(x)$的次数，记作 $\deg f(x)$. 对零多项式不定义次数. 只有常数项的多项式的次数等于 0. 并有

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

- **不可约多项式**：设 $f(x)\in D[x]^*$，若 $f(x)$不能分解为两个次数更低的多项式之积，则称 $f(x)$是一个不可约多项式. 也就是 $D[x]$中的不可约元.

2. $P[x]$中多项式的性质

设 $P=P(D)$是 D 上的分式域，$P[x]$也是惟一分解整环.

- $P[x]$中任何一个非零多项式(通过通分)可表示为一个本原多项式与一个非零元之积：

  $\forall f(x)\in P[x]^*$，$f(x)=r\varphi(x)$，其中 $r\in P^*$，$\varphi(x)\in D[x]$是本原多项式.
- 设 $f(x)\in D[x]^*$ 是本原多项式，则

$$f(x) \text{ 在 } D[x] \text{ 中不可约} \Leftrightarrow f(x) \text{ 在 } P[x] \text{ 中不可约}.$$
$$(f(x) \text{ 在 } D[x] \text{ 中可约} \Leftrightarrow f(x) \text{ 在 } P[x] \text{ 中可约}.)$$

3. $D[x]$、$P[x]$中多项式的可约性的判断方法

- 根与系数的关系：设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in D[x]$，$n\geqslant 1$，若 $f(x)$在 $P=P(D)$中有根$\dfrac{s}{r}$，$(r,s)\sim 1$，则 $r\mid a_n$，$s\mid a_0$.

该性质的意义是，通过分解 a_n 和 a_0 可找出所有的一次因子. 然后再用待定系数法确定是否可分解出 2 次因子，等等，从而判断多项式是否可约.

- 爱森斯坦定理：设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in D[x]$，$n\geqslant 1$，且是本原多项式. 若有既约元 $p\in D$ 满足：

(1) $p|a_i, i=0,1,\cdots,n-1$，但 $p\nmid a_n$；

(2) $p^2\nmid a_0$.

则 $f(x)$在 $D[x]$和 $P[x]$中不可约.

- 补充：有些多项式用爱森斯坦定理仍然解决不了，下面再给出几种方法：

  (1) 变换多项式，使其可用爱森斯坦定理.

$$f(x)\text{ 不可约} \Leftrightarrow f(x+k)\text{ 不可约}.$$

  (2) 简化系数：设 $\bar{f}(x)$为对 $f(x)$的系数作模 m 的运算所得之多项式，则

  $f(x)$ 可约 $\Rightarrow \bar{f}(x)$ 可约，或 $\bar{f}(x)$ 不可约 $\Rightarrow f(x)$ 不可约.

  (注意逆定理不成立.)

例 研究 $f(x)=x^5+x^3+3x^2-x+5$ 在$\mathbb{Z}[x]$中的可约性.

解 对多项式系数作模 2 的运算，得

$$\bar{f}(x) = x^5 + x^3 + x^2 + x + 1 \in Z_2[x],$$

因 $\bar{f}(1)\neq 0$，故 $\bar{f}(x)$无 1 次因子. 在 $Z_2[x]$中 2 次不可约多项式只有 x^2+x+1，经计算不能除尽 $\bar{f}(x)$，故 $\bar{f}(x)$在 $Z_2[x]$中不可约. 所以 $f(x)$在$\mathbb{Z}[x]$中不可约.

点评 以上做法比在$\mathbb{Z}[x]$中进行待定系数法简单得多. 因此对于低次的不可约多项式用模 m 的方法相当有效. 但若 $\bar{f}(x)$可约，就不能判断 $f(x)$是否可约了.

二、习题 3.6 详细解答

3.6-1 证明$\mathbb{Z}[x]$不是主理想整环.

分析 该题是复习主理想整环的概念. 要证明它不是主理想整环，只要找出一个理想不是主理想.

证 我们设法在$\mathbb{Z}[x]$中找出一个理想不是主理想.

取理想 $I=(2,x)$. 下面证明它不是主理想：

用反证法. 假设 I 是主理想，则存在 $f(x)\in\mathbb{Z}[x]$使

$$I = (2,x) = (f(x)).$$

则得 $f(x)|2$ 和 $f(x)|x$，因而有 $f(x)\sim 1$. 于是得到

$$I = (2,x) = (f(x)) = (1) = \mathbb{Z}[x].$$

因而存在 $u(x),v(x)\in\mathbb{Z}[x]$使

$$2u(x) + xv(x) = 1.$$

设 $u(x)=a_0+a_1x+\cdots+a_kx^k$，则得 $2a_0=1$，与 $a_0\in\mathbb{Z}$ 矛盾.

所以$\mathbb{Z}[x]$不是主理想整环.

点评 读者可找其他的理想不是主理想的例子.

3.6-2 设 D 是惟一分解整环，$P=P(D)$是 D 上的分式域. 证明：

(1) $P[x]$中任何一个非零多项式可表示为一个本原多项式与一个非零元之积：$\forall f(x)\in P[x]^*$，$f(x)=r\varphi(x)$，其中 $r\in P^*$，$\varphi(x)\in D[x]$是本原多项式.

(2) 设 $f(x)\in D[x]^*$ 是本原多项式，则

$$f(x)\text{ 在 }D[x]\text{ 中不可约}\Rightarrow f(x)\text{ 在 }P[x]\text{ 中不可约}.$$

(3) 设 $f(x)\in D[x]$是首1多项式，$g(x)$是 $f(x)$在 $P[x]$中的首1多项式因子，则 $g(x)\in D[x]$.

分析 这些结论都是比较显然的，主教材中一带而过. 为了熟悉多项式环，我们详细证明它们.

证 (1) 主要是通过对 $f(x)$的系数进行通分即可证明. 设

$$f(x)=\frac{b_n}{a_n}x^n+\cdots+\frac{b_1}{a_1}x+\frac{b_0}{a_0}\in P[x],$$

通分后得

$$\begin{aligned}f(x)&=\frac{1}{a_n\cdots a_1a_0}(c_nx^n+\cdots+c_1x+c_0)\\&=\frac{d}{a_n\cdots a_1a_0}(q_nx^n+\cdots+q_1x+q_0)\\&=r\varphi(x).\end{aligned}$$

其中 $d=(c_n,\cdots,c_1,c_0)$，$(q_n,\cdots,q_1,q_0)\sim1$，$r\in P^*$，$\varphi(x)\in D[x]$是本原多项式.

(2) 设 $f(x)\in D[x]^*$ 是本原多项式，则

$$f(x)\text{ 在 }D[x]\text{ 中不可约}\Rightarrow f(x)\text{ 在 }P[x]\text{ 中不可约}.$$

证 用反证法. 假设 $f(x)$在 $P[x]$中不可约，则 $f(x)$可表示为

$$f(x)=g(x)h(x),\quad g(x)\in P[x],\quad \deg g(x)\geqslant 0,$$
$$h(x)\in P[x],\quad \deg h(x)\geqslant 0.$$

由(1)，$g(x)$和 $h(x)$可表示为

$$g(x)=r\varphi(x),\quad h(x)=s\psi(x),$$

其中 $r,s\in P^*$，$\varphi(x),\psi(x)\in D[x]$且是本原多项式. 故有

$$f(x)=rs\varphi(x)\psi(x)=\frac{b}{a}\varphi(x)\psi(x),\quad a,b\in D,\quad (a,b)\sim1.$$

由于两个本原多项式之积仍为本原多项式，故 $\varphi(x)\psi(x)$是本原多项式. 又由

$af(x)=b\varphi(x)\psi(x)$两边的系数的最大公因子相伴，得 $a\sim b$，即 $b=ua$，$u\in U(D)$，所以 $f(x)=u\varphi(x)\psi(x)$，即 $f(x)$在 $D[x]$中可约，矛盾.

(3) 设 $f(x)\in D[x]$是首 1 多项式，$g(x)$是 $f(x)$在 $P[x]$中的首 1 多项式因子，则 $g(x)\in D[x]$.

证 由于 $f(x)\in D[x]$是首 1 多项式，也是本原多项式. 设

$$f(x)=g(x)h(x),\quad g(x)\in P[x],\quad \deg g(x)\geqslant 0,$$
$$h(x)\in P[x],\quad \deg h(x)\geqslant 0,$$

其中 $g(x)$是首 1 多项式.

显然 $h(x)$也是首 1 多项式. $g(x)$可表示为

$$g(x)=r\varphi(x),$$

其中 $r\in P^*$，$\varphi(x)\in D[x]$且是本原多项式.

比较首项系数，设 $\varphi(x)\in D[x]$的首项系数为 b_m，则得 $rb_m\sim 1$，因而 $r\sim 1$，$b_m\sim 1$，所以 $g(x)\in D[x]$.

点评 虽然这些结论都是比较显然的，但证明起来并不简单，值得思考.

3.6-3 若 D 是有单位元的整环但不是域，则 $D[x]$不是主理想整环.

分析 联想到$\mathbb{Z}[x]$不是主理想整环的证明，能否用类似方法证明此题.

证 用反证法. 假设 D 是主理想整环. 任取 $a\in D^*$，考虑理想(a,x)，由于 D 是主理想整环，故存在 $f(x)\in D[x]$使$(a,x)=(f(x))$. 由 $f(x)\mid a$ 和 $f(x)\mid x$，得 $f(x)\sim 1$，因而有 $b\in D$，$u(x)\in D[x]$使 $ab+xu(x)=1$. 比较两边系数得 $ab=1$，a 是可逆元，由于 a 是 D^* 中任取的，所以 D 是域，与已知条件矛盾. 从而证明了 $D[x]$不是主理想整环.

点评 方法类似$\mathbb{Z}[x]$不是主理想整环的证明.

3.6-4 判断下列多项式在$\mathbb{Q}[x]$中是否可约？

(1) x^4+1.

(2) x^p+px+1，p 为素数.

(3) $f(x)=x^5+x^3+3x^2-x+1$.

分析 如本节内容提要中指出，判断一个整数系数多项式在$\mathbb{Q}[x]$中是否可约的方法有以下几种：(1)用试根法判断是否有一次因子. (2)用爱森斯坦定理. (3)将多项式变形后再用爱森斯坦定理. (4)待定系数法. (5)对多项式系数作模 2 的运算，在 $Z_2[x]$中考虑问题. 等等.

解 (1) 直接用爱森斯坦定理不好用，所以我们对它变一下形，考虑多项式：

$$f(x+1)=x^4+4x^3+6x^2+4x+2,$$

由爱森斯坦定理，取 $p=2$，知 $f(x+1)$在$\mathbb{Q}[x]$中不可约，所以 $f(x)$在$\mathbb{Q}[x]$

中不可约.

点评　此题用待定系数法也不难.首先由于 $f(x)$ 在 $\mathbb{Z}$ 中的根只能是 1 或 -1,代入后都不是,所以 $f(x)$ 在 $\mathbb{Z}[x]$ 中无一次因子. $f(x)$ 在 $\mathbb{Z}[x]$ 中 2 次因子只能是 x^2+ax+1 或 x^2+ax-1.设 $x^4+1=(x^2+ax+1)(x^2+bx+1)$,比较两边系数得方程: $a+b=0, ab+2=0$,在 $\mathbb{Z}$ 中无解.所以 $f(x)$ 在 $\mathbb{Z}[x]$ 中无 2 次因子.综上, $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

看来用待定系数法比用爱森斯坦定理还是麻烦一些.

(2) 分两种情况来讨论:

情况 1: $p=2$.显然是可约的.

情况 2: $p>2$.对多项式变形,考虑 $f(x-1)$,由于

$$f(x-1)=x^p-px^{p-1}+\cdots+2px-p,$$

由爱森斯坦定理知 $f(x-1)$ 在 $\mathbb{Q}[x]$ 中不可约,所以 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

(3) **分析**　首先我们大致看一下,不能直接用爱森斯坦定理,变形也困难.与前面在内容提要中的例子相近,该多项式极有可能不可约,可在 $Z_2[x]$ 中进行.

证　对多项式系数作模 2 的运算,得

$$\bar{f}(x)=x^5+x^3+x^2+x+1\in Z_2[x],$$

因 $\bar{f}(1)\neq 0$,故 $\bar{f}(x)$ 无 1 次因子.在 $Z_2[x]$ 中 2 次不可约多项式只有 x^2+x+1,经计算不能除尽 $\bar{f}(x)$,故 $\bar{f}(x)$ 无 2 次因子.综上, $\bar{f}(x)$ 在 $Z_2[x]$ 中不可约,所以 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约.

点评　对于低次多项式的可约性问题,一般来说比较容易,有一个待定系数法垫底,不会很复杂.

3.6-5　写出 $Z_3[x]$ 中全部次数 $\leqslant 3$ 的首 1 不可约多项式.

分析　我们前面已经用到过 $Z_2[x]$ 中多项式问题,由于 $Z_n[x]$ 中 k 次多项式的个数是有限的,可以全部找出,因而可从中挑出那些不可约多项式.以后我们将给出计算不可约多项式的个数的方法,从而可以有指导地解决问题.

解　用枚举法求出:

1 次不可约多项式: $x, x+1, x+2$.

2 次不可约多项式: x^2+1, x^2+x+2, x^2+2x+2.

3 次不可约多项式: $x^3+2x+1, x^3+2x+2, x^3+2x^2+1, x^3+x^2+2$,

$$x^3+x^2+x+2,\quad x^3+x^2+2x+1,$$

$$x^3+2x^2+x+1,\quad x^3+2x^2+2x+2.$$

共 14 个不可约多项式.

点评 对 3 次以下的多项式只需用试根法就可判定.

3.7 应用举例

一、内容提要

环的应用是多方面的,我们这里主要介绍在编码问题上的应用.首先要搞清"编码问题"与"密码问题"的区别."编码问题"研究的是怎样用数字来表达信息,便于接受方收到信息后,能检查出错误或纠正错误.解决此问题的一个简单的方法是用所谓"距离码",即表达信息的数码等距地分布在一个数列中,因此当接收到的数码不在信息码范围内时,就说明此信息有错;如果距离为偶数个数码,则可认为最靠近的信息码是所要的信息.

本节介绍多项式检错码,为了说得清楚,要规范一些名词.

1. 名词

信息码:表示信息的(二进制)数字,设为 k 位.

检验码:用于检测错误的数字,设为 h 位.

码词:信息码+检验码,设为 $n=h+k$ 位.称为(n,k)—码.

2. 多项式检验码的编码方法

(1) 确定码词长度 n 与信息码长度 k.

(2) 在 $Z_2[x]$中选定一个 $n-k$ 次多项式 $p(x)$作为检验多项式(或称生成多项式,用它来生成码词,与理想中的生成元的概念不同.)$p(x)$不要求不可约,但也不能太简单.

(3) 对每一个 k 位信息,可得到一个信息码多项式 $m(x)$(它的次数最高为 $k-1$).

(4) 作带余除法:$x^{n-k}m(x)=q(x)p(x)+r(x)$,得到 $r(x)$.

(5) 码词多项式为:$v(x)=x^{n-k}m(x)+r(x)(=q(x)p(x))$(它的次数最高为 $n-1$).

检错方法:把接收到的码词多项式用 $p(x)$作带余除法,若除尽,则接收到的信息是正确的,否则有误.

二、习题 3.7 详细解答

3.7-1 写出由 $p(x)=1+x^2+x^3$ 生成的所有(6,3)码.

分析 按内容提要的步骤进行计算.

解 作下表：

信息	信息多项式 $m(x)$	$x^3m(x)$	$r(x)$：$x^3m(x)=q(x)p(x)+r(x)$	$v(x)=r(x)+x^3m(x)$	码词
000	0	0	0	0	000000
100	1	x^3	$1+x^2$	$1+x^{2+}\ x^3$	101100
010	x	x^4	$1+x+x^2$	$1+x+x^2+x^4$	111010
001	x^2	x^5	$1+x$	$1+x+x^5$	110001
110	$1+x$	x^3+x^4	x	$x+x^3+x^4$	010110
101	$1+x^2$	x^3+x^5	$x+x^2$	$x+x^2+x^3+x^5$	011101
011	$x+x^2$	x^4+x^5	x^2	$x^2+x^4+x^5$	001011
111	$1+x+x^2$	$x^3+x^4+x^5$	1	$1+x^3+x^4+x^5$	100111

3.7-2 检验下列接收到的码词是否正确？生成多项式为 $p(x)=1+x^2+x^3+x^4$.

(1) 10011011，(2) 01110010，(3) 10110101 .

解 (1) $u(x)=1+x^3+x^4+x^6+x^7$，$p(x)$不能整除 $u(x)$，故有错.

(2) $u(x)=1+x^2+x^3+x^6$，$p(x)$能整除 $u(x)$，故正确.

(3) $u(x)=1+x^2+x^3+x^5+x^7$，$p(x)$不能整除 $u(x)$，故有错.

第 3 章补充题

补充题 3-1 用同态基本定理证明：$\mathbb{Z}[\mathrm{i}]/(3+\mathrm{i})\cong(Z_{10},+,\cdot)$.

分析 对此题同态映射并不显然，所以我们首先要在确定$\mathbb{Z}[\mathrm{i}]$到 Z_{10} 的同态映射上花费一些工夫.

证 设 $Z_{10}=\{\overline{0},\overline{1},\cdots,\overline{9}\}$，设 φ 是$\mathbb{Z}[\mathrm{i}]$到 Z_{10} 的满同态映射，则有 $\varphi(1)=\overline{1}$，由于元素 i 是$\mathbb{Z}[\mathrm{i}]$的生成元，确定了它的像就决定了同态映射. 可设 $\varphi(\mathrm{i})=\overline{k}$，则由 $\varphi(\mathrm{i}^2)=\varphi(-1)=\overline{k^2}=-\overline{1}$，得二次同余方程$\overline{k^2}=\overline{9}$ 的解 $k=3$ 或 $k=-3$. 取 $k=-3$，则得到 φ 的表达式：

$$\varphi(a+b\mathrm{i})=\overline{a-3b}(\mathbb{Z}[\mathrm{i}]\to Z_{10}).$$

下面证明 φ 是同态：

$$\begin{aligned}\varphi(a+b\mathrm{i}+c+d\mathrm{i})&=\varphi(a+c+(b+d)\mathrm{i})=a+c-3(b+d)\\&=\varphi(a+b\mathrm{i})+\varphi(c+d\mathrm{i}),\\\varphi((a+b\mathrm{i})(c+d\mathrm{i}))&=\varphi((ac-bd)+(ad+bc)\mathrm{i})\\&=\overline{(ac-bd)-3(ad+bc)},\\\varphi(a+b\mathrm{i})\varphi(c+d\mathrm{i})&=\overline{(a-3b)(c-3d)}=\overline{ac+9bd-3(bc+ad)}\end{aligned}$$

$$= \overline{ac - bd - 3(bc + ad)},$$

故 $\varphi((a+bi)(c+di))=\varphi(a+bi)\varphi(c+di)$.

且易证 φ 是满同态. 求核:

$$\begin{aligned}\ker \varphi &= \{a + bi \mid \overline{a - 3b} = \overline{0}\} = \{a + bi \mid \overline{a} = \overline{3b}\} \\ &= \{a + bi \mid a = 3b + 10q, q \in \mathbb{Z}\} \\ &= \{3b + bi + 10q \mid b, q \in \mathbb{Z}\} \\ &= \{(3 + i)b + (3 + i)(3 - i)q \mid b, q \in \mathbb{Z}\} \\ &= \{(3 + i)(b + 3q - qi) \mid b, q \in \mathbb{Z}\} \\ &= \{(3 + i)x \mid x \in \mathbb{Z}[i]\} = (3 + i).\end{aligned}$$

所以由同态基本定理得

$$\mathbb{Z}[i]/(3 + i) \equiv (Z_{10}, +, \cdot).$$

点评 研究一下在确定同态映射的过程中,能否取 $k=3$?

补充题 3-2 用同态基本定理证明: $\mathbb{Z}[i]/(5)\equiv(Z_5,+,\cdot)\times(Z_5,+,\cdot)$.

分析 首先注意左边的理想(5)并非 $\{5q \mid q\in\mathbb{Z}\}$,而是 $(5)=\{5(a+bi)\mid a,b\in\mathbb{Z}\}$. 右边的乘法是笛卡儿积. 我们首先要确定 $\mathbb{Z}[i]$ 到 $Z_5\times Z_5$ 的一个同态映射.

证 设 φ 是 $\mathbb{Z}[i]$ 到 $Z_5\times Z_5$ 的满同态映射. 关键是确定元素 i 的像. 根据前面 3.3 节内容提要中的例子,可令 $\varphi(i)=(\overline{k_1},\overline{k_2})$,取 $k_1=-2, k_2=2$,则得

$$\varphi(a + bi) = (\overline{a - 2b}, \overline{a + 2b}).$$

易证 φ 保持运算,显然是满射. 计算核:

$$\begin{aligned}\ker\varphi &= \{a + bi \mid \overline{a - 2b} = \overline{0} \,\&\, \overline{a + 2b} = \overline{0}\} \\ &= \{a + bi \mid \overline{a} = \overline{0} \,\&\, \overline{b} = \overline{0}\} \\ &= \{5s + 5ti \mid s, t \in \mathbb{Z}\} = (5).\end{aligned}$$

所以由同态基本定理得

$$\mathbb{Z}[i]/(5) \equiv (Z_5, +, \cdot) \times (Z_5, +, \cdot).$$

点评 事实上我们已经得到过 $\mathbb{Z}[i]/(2+i)\equiv(Z_5,+,\cdot)$ 和 $\mathbb{Z}[i]/(2-i)\equiv(Z_5,+,\cdot)$,两边作笛卡儿积,也可证明此结果.

补充题 3-3 设 α 是 $\mathbb{Z}[i]$ 中的既约元,则 α 能且只能整除一个素数.

分析 利用元素的范数来讨论此问题.

证 设 $\alpha=a+bi, v(\alpha)=\alpha\overline{\alpha}=a^2+b^2=p_1\cdots p_s, p_j(j=1,2,\cdots,s)$ 为素数. 由 $\mathbb{Z}[i]$ 的惟一分解性知, α 是素元,故必有某个 p_k 使 $\alpha \mid p_k$.

再证惟一性: 如果 α 是素数,则显然成立. 下设 α 是真复数: $\alpha=a+bi$,

$ab\neq 0$. 设 $\alpha\mid p$，p 是素数. 则有 $\bar{\alpha}\mid p$. 因为 α 是既约元，因而 $(\alpha,\bar{\alpha})\sim 1$ 和 $\alpha\bar{\alpha}\mid p$，于是有 $p=\alpha\bar{\alpha}$，所以 p 由 α 惟一确定.

点评 这个结果说明了一个真复数如果是素元，其范数必为素数.

补充题 3-4 证明高斯整数环 $\mathbb{Z}[\mathrm{i}]$ 中全部既约元为

(1) $\{p\mid p$ 是素数且 $p\neq a^2+b^2,\ \forall a,b\in\mathbb{Z}^+\}=\{p\mid p$ 是素数且 $p\equiv 3(\mathrm{mod}\ 4)\}$；

(2) $\{a+b\mathrm{i}\mid a^2+b^2=p$(素数)$\}$.

分析 首先 $\mathbb{Z}[\mathrm{i}]$ 中的元素可分三类：整数 a，纯虚数 $b\mathrm{i}$，真复数 $a+b\mathrm{i}$，$ab\neq 0$. 因 $U(\mathbb{Z}[\mathrm{i}])=\{1,-1,\mathrm{i},-\mathrm{i}\}$，纯虚数与整数是相伴的，所以我们只要分析两类元素：整数和真复数. 而整数又只需分析素数，故分以下两种情况：

(1) 设 p 是素数，则 p 是既约元 $\Leftrightarrow p\neq a^2+b^2,\ \forall a,b\in\mathbb{Z}^+$.

(2) 设 $\alpha=a+b\mathrm{i}$，且 $ab\neq 0$，$(a,b)=1$，则 α 是既约元 $\Leftrightarrow a^2+b^2=p$(素数).

证 充分性：设 p 是既约元，要证 $p\neq a^2+b^2,\ \forall a,b\in\mathbb{Z}^+$.

(1) 反证法：假设 $\exists\, a,b\in\mathbb{Z}^+ : p=a^2+b^2$，则 $p=(a+b\mathrm{i})(a-b\mathrm{i})$，且 $ab\neq 0$，$(a,b)=1$，因而 $a+b\mathrm{i}$ 和 $a-b\mathrm{i}$ 都不是可逆元，与 p 是既约元矛盾.

必要性：设 $p\neq a^2+b^2,\ \forall a,b\in\mathbb{Z}^+$，要证 p 是既约元.

用反证法. 假设 p 不是既约元，则 $p=\alpha\beta$，α,β 都不是可逆元. 可设 $\alpha=a+b\mathrm{i}$ 是既约元. 由 $p=\bar{\alpha}\bar{\beta}$ 得 $(a-b\mathrm{i})\mid p$. 因为 $a+b\mathrm{i}$ 与 $a-b\mathrm{i}$ 都是既约元，$(a+b\mathrm{i},a-b\mathrm{i})\sim 1$. 故 $(a+b\mathrm{i})(a-b\mathrm{i})\mid p$，因而有 $p=(a+b\mathrm{i})(a-b\mathrm{i})q$，考虑到 p 是素数，所以 $p=(a+b\mathrm{i})(a-b\mathrm{i})=a^2+b^2$，矛盾.

(2) 充分性：设 $\alpha=a+b\mathrm{i}$ 是既约元，要证 $a^2+b^2=p$(素数).

用反证法. 假设 $a^2+b^2=qr$，$q>1$，$r>1$ 且 q 为素数. 因 $\alpha=a+b\mathrm{i}$ 是既约元，可设 $\alpha\mid q$，同时有 $\bar{\alpha}\mid q$，于是得 $a^2+b^2=q$，与 $r>1$ 矛盾. 所以 a^2+b^2 必为素数.

必要性：设 $a^2+b^2=p$(素数)，要证 $\alpha=a+b\mathrm{i}$ 是既约元.

用反证法. 假设 $\alpha=a+b\mathrm{i}$ 不是既约元. 可设 $\alpha=\beta\gamma$，且 $\beta,\gamma\notin U(\mathbb{Z}[\mathrm{i}])$，则 $a^2+b^2=v(\alpha)=v(\beta)v(\gamma)$，且 $v(\beta)>1$，$v(\gamma)>1$，与 $a^2+b^2=p$(素数)矛盾.

点评 这是一个很重要的结果，对高斯整数环内的素元作出一个终结性的结果.

第 4 章 域 论

域是特殊的环，它是我们平时经常在做的＋，－，×，÷四则运算的对象. 有理数集合，实数集合，复数集合对普通加法和乘法都构成域. 但有一类域是平常不大意识到的，这就是有限域，它在数字通信中特别重要，是这一章的重点.

4.1 域和域的扩张，几何作图问题

一、内容提要

1. 域$(F,+,\cdot)$的定义

(1)$(F,+,\cdot)$是非零环，(2)$(F^*,\cdot)$是可换群. 用一句话来表达就是：非零元都可逆的非零可换环.

一些已知的重要的例：

(1) 数域：$(\mathbb{Q},+,\cdot)$，$(\mathbb{R},+,\cdot)$，$(\mathbb{C},+,\cdot)$等.

(2) $Z_2=\{0,1\}$，$(Z_2,+,\cdot)$是元素最少的域，运算是模 2 的加法和乘法，加法：$1+1=0$，$-1=1$；乘法：$1\cdot 1=1$，$1^{-1}=1$. 在数字计算与通信中特别重要.

(3) $(Z_p,+,\cdot)$，p 是素数. $Z_p=\{\bar{0},\bar{1},\cdots,\overline{p-1}\}$，运算是模 p 的加法和乘法. 有时为了书写简单，写成：$Z_p=\{0,1,\cdots,p-1\}$，运算结果取正则代表元. 负元：$-k=p-k$，逆元的计算比较复杂：设 $k\in Z_p^*$，$ks+pt=1$，则 $k^{-1}=s(\bmod p)$.

2. 域的特征：

- 域$(F,+,\cdot)$的特征：域中单位元 1 的加法阶 $o^+(1)$或等于素数 p，或等于∞. 当 $o^+(1)=p$(素数)时，域的特征 $\mathrm{ch}F=p$；当 $o^+(1)=\infty$时，域的特征 $\mathrm{ch}F=0$.

F 是有限域时，$\mathrm{ch}F=p$. 但反之，当 $\mathrm{ch}F=p$ 时，F 可以是有限域，也可以是无限域.

- 特征为 p 的域 F 内元素运算的性质：$\forall a,b\in F$ 有

  (1) $\forall a\in F$，$pa=0$；

  (2) $na=ma(a\neq 0)\Rightarrow n\equiv m(\bmod p)$；

(3) $e\geqslant 0$，整数，$(a\pm b)^{p^e}=a^{p^e}\pm b^{p^e}$.

- 素域：由元素1生成的子域称为素域，记作 F_0. 当 $o^+(1)=p$ 时，$F_0=\langle 1\rangle=Z_p$；当 $o^+(1)=\infty$ 时，$F_0=\langle 1\rangle=\mathbb{Q}$.

3. 域的扩张

- 域的扩张次数：设 F 是 E 的子域，记作 $F\leqslant E$ 或 $E|F$（注意此记号与整除记号相同，不要搞混）. E 可看作为 F 上的线性空间，用线性代数中常用的记号记作 $E(F)$，$E(F)$ 的维数称为 E 对 F 的扩张次数，记作 $(E:F)=\dim E(F)$.
- 扩张次数满足望远镜公式：设 $F\leqslant K\leqslant E$ 为有限扩张，则 $(E:F)=(E:K)(K:F)$.
- 代数元（数）与超越元（数）：设 $u\in E|F$，若 u 是 F 上某个多项式的根，则称 u 是 F 上的代数元，否则称 u 是 F 上的超越元. $\mathbb{Q}$ 上的代数元称为代数数，$\mathbb{Q}$ 上的超越元称为超越数. 当 u 是 F 上的代数元时，若 u 的最小多项式次数为 r，则称 u 是 F 上的 r 次代数元.（所谓元素 u 的**最小多项式**，指以 u 为一个根 F 上的次数最低的首1多项式.）
- 代数扩张与超越扩张：设 $E|F$，若 E 中的元素都是 F 上的代数元，则称 E 是 F 的代数扩张，否则称 E 是 F 的超越扩张.
- 添加元素的扩张：设 $S\subset E|F$，$F(S)$ 为包含 F 与 S 的最小域，称为 F 添加 S 的扩张域. 添加一个元素 $u\in E|F$ 的扩张称为单扩张，单扩张 $F(u)$ 的结构如下：

(1) 当 u 是 F 上的 n 次代数元时，设 u 的最小多项式为 $p(x)$，则

$$F(u)=\{a_0+a_1u+\cdots+a_{n-1}u^{n-1}\mid a_0,a_1,\cdots,a_{n-1}\in F\}\cong F[x]/(p(x)),$$

且 $(F(u):F)=n$.

(2) 当 u 是 F 上的超越元时，则

$$\begin{aligned}F(u)&=\left\{\frac{f(u)}{g(u)}\mid f(x),g(x)\in F[x],g\neq 0\right\}\\&=\left\{\frac{f(x)}{g(x)}\mid f(x),g(x)\in F[x],g\neq 0\right\},\end{aligned}$$

且 $(F(u):F)=\infty$.

4. 域的代数扩张的性质

- 设 $a,b\in E|F$，$(F(a):F)=m$，$(F(b):F)=n\Rightarrow(F(a,b):F)\leqslant mn$.
- 设 $a,b\in E|F$ 是 F 上的代数元，则 $a\pm b$，ab，$a/b(b\neq 0)$ 是 F 上的代数元.
- 代数扩张与有限扩张的关系：$E|F$ 是有限扩张，则 $E|F$ 是代数扩张.

5. 几何作图问题

问题提法:已知平面上点(0,0)和(1,0),用圆规和无标记的直尺可作出哪些点?可用圆规和无标记的直尺作出的点的坐标称为可构造数.

- 可构造数的充分必要条件:实数 α 可构造的充分必要条件是存在有限域链
$$K_0 = Q \leqslant K_1 \leqslant \cdots \leqslant K_n$$
满足 $(K_i:K_{i-1})=2, i=1,\cdots,n$ 和 $\alpha \in K_n$.
- 三等分任意角问题的解:已知角 φ 和 $\cos\varphi$,则 φ 可(用园规和直尺)三等分的充分必要条件是多项式
$$\psi(x) = 4x^3 - 3x - \cos\varphi$$
在 $Q(\cos\varphi)$ 上可约. 而 3 次多项式的可约性可用试根法完全解决,所以某个角是否可三等分的问题也完全解决.

例 取 $\varphi=60^\circ$, $\psi(x)=4x^3-3x-\dfrac{1}{2}=\dfrac{1}{2}(8x^3-6x-1)$ 在 $\mathbb{Q}(\cos\varphi)=\mathbb{Q}$ 上不可约,所以 $\varphi=60^\circ$ 不能三等分.

- 正 p 边形可作出的必要条件:设 p 是素数,则正 p 边形可作出的必要条件是 p 是如下形式的费尔马素数:
$$p = 2^{2^m} + 1, \quad m \geqslant 0 \text{ 整数}.$$

例 $p=7,11,13$ 都不是费尔马素数,所以相应的正 P 边形都不能作出.

二、习题 4.1 详细解答

4.1-1 设 F 是域, $\mathrm{ch}F=p$(素数), $a,b\in F$,证明:

(1) $na=ma(a\neq 0)\Rightarrow n\equiv m(\mathrm{mod}\ p)$;

(2) $e\geqslant 0$ 整数, $(a\pm b)^{p^e}=a^{p^e}\pm b^{p^e}$.

分析 该题主要目的是熟悉域的特征及域内的运算性质.

证 (1) $na=ma(a\neq 0)$,由消去律得 $m1=n1$(注意不能得到 $m=n$),于是有 $(m-n)1=0$. 因为 $o^+(1)=p$,故由阶的性质得到 $p\mid(m-n)$,所以 $n\equiv m(\mathrm{mod}\ p)$.

点评 乘法消去律两边消去相同元素后,剩下的应是元素,而整数 m 与 n 并不是 F 中的元素,所以由 $na=ma(a\neq 0)$ 并不能得到 $m=n$. 正确的做法应将式子表示为 $(n1)\cdot a=(m1)\cdot a(a\neq 0)$,然后两边消去 a,得到 $m1=n1$.

(2) 对 e 作归纳法. $e=0$ 显然成立. 下设 $e\geqslant 1$.

为了叙述简化,我们对 $e=1$ 的情况单独证明一下:

$$(a\pm b)^p = a^p \pm pa^{p-1}b + \cdots + (-1)^k \frac{p(p-1)\cdots(p-k+1)}{k!}$$
$$\cdot a^{p-k}b^k + \cdots \pm b^p,$$

由于$(k!) \mid p(p-1)\cdots(p-k+1)$，且$(k!,p)=1$，故有$(k!) \mid (p-1)\cdots(p-k+1)$.因而

$$\frac{p(p-1)\cdots(p-k+1)}{k!} \equiv 0 (\bmod p), \quad 1 \leqslant k \leqslant p-1.$$

所以$(a\pm b)^p = a^p \pm b^p$.

假设公式对 $e-1$ 成立，要证对 e 成立.

$$(a\pm b)^{p^e} = [(a\pm b)^{p^{e-1}}]^p (\text{用归纳假设}) = [a^{p^{e-1}} \pm b^{p^{e-1}}]^p = a^{p^e} \pm b^{p^e}.$$

所以公式对任何非负整数 e 都成立.

点评 如果不用 $e=1$ 的公式过渡一下，直接用归纳法，书写比较复杂，读者不妨自己试一下.

4.1-2 设$\mathbb{Z}[\mathrm{i}]$是高斯整数环，求域$\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})$的特征.

分析 根据域的特征的定义，就是域中单位元的加法阶.

解 首先把域的元素表达出来：

$$\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i}) = \{a+b\mathrm{i}+(2+\mathrm{i}) \mid a,b \in \mathbb{Z}\} = \{\overline{a+b\mathrm{i}} \mid a,b \in \mathbb{Z}\}.$$

考虑 $\bar{1}$ 的加法阶. 因为 $5=(2+\mathrm{i})(2-\mathrm{i})$，故 $\bar{5}=\bar{0}$，所以

$$o^+(\bar{1}) = 5, \quad \mathrm{ch}[\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})] = 5.$$

点评 也可直接利用前面已经得到的结果：$\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i}) \cong (Z_5, +, \cdot)$.

4.1-3 设 p 为素数，$(n,p)=1$，则 $n^{p-1} \equiv 1 (\bmod p)$.

分析 此结果已在群论中证明过(见主教材定理 2.5.4 及其推论)，我们只是从域的角度再证明一下.

证 考虑域$(Z_p, +, \cdot)$中的乘群$(Z_p^*, \cdot)$，因为$(n,p)=1$，所以 $\bar{n} \neq \bar{0}$，因而 $\bar{n} \in Z_p^*$. 由$|Z_p^*| = p-1$ 和乘群的阶的性质，得到 $\bar{n}^{p-1} = \bar{1}$，所以

$$n^{p-1} \equiv 1 (\bmod p).$$

点评 条件$(n,p)=1$ 是排除 $\bar{n}=\bar{0}$ 的情形.

4.1-4 设 $F \leqslant K \leqslant E$，且为有限扩张，则$(E:F)=(E:K)(K:F)$.

分析 此公式类似于群论中的望远镜公式，可以说是域的扩张次数的望远镜公式，其证明方法需根据扩张次数的定义.

证 由扩张次数的定义，它是线性空间的维数.

设$(E:K)=m$，且线性空间 $E(K)$的一组基为：$u_1, u_2, \cdots, u_m$；设$(K:F)=n$，

且线性空间 $K(F)$ 的一组基为：$v_1,v_2,\cdots,v_n$. 易证 $u_iv_j, i=1,2,\cdots,m; j=1,2,\cdots,n$ 是线性空间 $E(F)$ 的一组基(略). 所以 $(E:F)=mn=(E:K)(K:F)$.

点评 同学做作业时，应把 $u_iv_j, i=1,2,\cdots,m; j=1,2,\cdots n$ 是线性空间 $E(F)$ 的一组基的证明过程详细写一下. 因为完全是"例行公事"式的证明，在本习题解答中就不必列出了.

4.1-5 设扩域 $K|F$，$a,b\in K$ 分别是 F 上的 m 次和 n 次代数元，证明 $(F(a,b):F)\leqslant mn$，且当 $(m,n)=1$ 时等式成立.

分析 本题的目的是熟悉代数元的次数的概念.

证 由于 a 是 F 上的 m 次代数元，可设它的最小多项式为

$$f(x)=x^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0\in F[x],$$

由于 b 是 F 上的 n 次代数元，可设它的最小多项式为

$$g(x)=x^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0\in F[x].$$

令 $E=F(a)$，则 $(E:F)=m$. 由于 $g(x)$ 也可看作是 E 上的多项式，但不一定不可约，因而 $(E(b):E)\leqslant n$. 由 $F(a,b)=E(b)$ 和域的望远镜公式，得

$$(F(a,b):F)=(F(a,b):F(a))(F(a):F)=(E(b):E))(E:F)\leqslant mn.$$

现证第二个结论：首先令 $(F(a,b):F)=k$，由前面的证明知 $k\leqslant mn$.

再由前面的证明有 $k=(F(a,b):F)=(F(a,b):F(a))(F(a):F)=(E(b):E)m$，因而 $m|k$；类似可得 $n|k$. 又由于 $(m,n)=1$，故有 $mn|k$ 和 $mn\leqslant k$.

综上，得 $k=mn$.

点评 用本题的结论可证明以下结果：

(1) a,b 是 F 上的代数元，则 $a\pm b, ab, \frac{a}{b}(b\neq 0)$ 都是 F 上的代数元.

证明此结果不必对每个表达式找出它所满足的多项式，可利用本题结果和有限扩张也是代数扩张的结论统一解决：设 $(F(a):F)=m$，$(F(b):F)=n$，$(F(a,b):F)\leqslant mn$，所以 $F(a,b)$ 是有限扩张，因而也是代数扩张. 而 $a\pm b, ab, \frac{a}{b}(b\neq 0)\in F(a,b)$，故 $a\pm b, ab, \frac{a}{b}(b\neq 0)$ 都是代数元.

(2) 在 F 上添加有限个代数元的扩张是有限扩张.

(3) E 是 F 上的代数扩张，K 是 E 上的代数扩张，则 K 是 F 上的代数扩张.

4.1-6 设 $\mathbb{Q}$ 为有理数域，

(1) 求 $u\in\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$ 使 $\mathbb{Q}(u)=\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$；

(2) 求 $w\in\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$ 使 $\mathbb{Q}(w)\neq\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$ 的条件是什么？

分析 本题涉及如何把一个添加有限个元素的扩张域表示为单扩张的方

法. 通常找一个次数等于扩张次数的代数元,并加以严格的证明.

解 (1) 由于$(\mathbb{Q}(\sqrt{2},\sqrt[3]{5}):\mathbb{Q})=6$,我们可取$u=\sqrt{2}\sqrt[3]{5}$.

显然,$u\in\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$,因而$\mathbb{Q}(u)\subseteq\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$.

反之,由于$u^3=10\sqrt{2}$,得$\sqrt{2}\in\mathbb{Q}(u)$;$u^4=20\sqrt[3]{5}$,得$\sqrt[3]{5}\in\mathbb{Q}(u)$,所以$\mathbb{Q}(\sqrt{2},\sqrt[3]{5})\subseteq\mathbb{Q}(u)$.

综上,得$\mathbb{Q}(u)=\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$.

(2) 由于$\mathbb{Q}(w)\subseteq\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$,$(\mathbb{Q}(\sqrt{2},\sqrt[3]{5}):\mathbb{Q})=6$,要使$\mathbb{Q}(w)\neq\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$必有$(\mathbb{Q}(w):\mathbb{Q})<6$. 但子域的扩张次数是扩域的扩张次数的因子,故$(\mathbb{Q}(w):\mathbb{Q})=1$,或2,或3.

所以

$$w=a+b\sqrt{2},\quad a,b\in\mathbb{Q},$$

或

$$w=a+b\sqrt[3]{5}+c\sqrt[3]{25},\quad a,b,c\in\mathbb{Q}.$$

点评 本题只对具体的例子给出单扩张的方法,显然,在(1)中元素的形式不是惟一的,例如取$u=\sqrt{2}+\sqrt[3]{5}$也可以. 我们将在下一节给出一般的方法.

4.1-7 设整数m_1,m_2,$(m_1,m_2)=1$,若m_1,m_2边形可作出,则m_1m_2边形也可作出.

分析 这是一个作图问题,由于我们目前只学了一个必要条件,所以还不能用定理来证明结论,只能具体问题具体分析,找出作图的方法.

证 在复平面上分析. 由于若m_1,m_2边形可作出,因而点$\mathrm{e}^{\frac{2\pi}{m_1}\mathrm{i}}$和点$\mathrm{e}^{\frac{2\pi}{m_2}\mathrm{i}}$可作出. 由$(m_1,m_2)=1$和最大公因子定理,存在整数$p$与$q$使$pm_1+qm_2=1$,做下列运算:

$$(\mathrm{e}^{\frac{2\pi\mathrm{i}}{m_1}})^q+(\mathrm{e}^{\frac{2\pi\mathrm{i}}{m_2}})^p=\mathrm{e}^{\frac{2(pm_1+qm_2)\pi\mathrm{i}}{m_1m_2}}=\mathrm{e}^{\frac{2\pi}{m_1m_2}\mathrm{i}},$$

说明点$\mathrm{e}^{\frac{2\pi}{m_1m_2}\mathrm{i}}$可作出,即$m_1m_2$边形可作出.

点评 圆周可n等分的充要条件将在4.4节中介绍. 我们不妨把书翻到4.4节定理4.4.4,:圆周可n等分的充要条件是$n=2^rp_1p_2\cdots p_s$,其中$p_k,k=1,2,\cdots,s$为不同的费尔马素数. 下面提前用一下该定理来证明本题.

由于m_1边形可作出,则m_1可表示为$m_1=2^rp_1p_2\cdots p_s$,其中$p_k,k=1,2,\cdots,s$为不同的费尔马素数. 由于m_2边形可作出,则m_2可表示为$m_2=2^hq_1q_2\cdots q_t$,其中$q_k,k=1,2,\cdots,t$为不同的费尔马素数. 于是得

$$m_1m_2 = 2^{r+h}p_1p_2\cdots p_sq_1q_2\cdots q_t,$$

由于$(m_1,m_2)=1$,因而 $p_1p_2\cdots p_sq_1q_2\cdots q_t$ 是互不相同的费尔马素数,所以 m_1m_2 边形可作出.

4.1-8　证明72°角可三等分.

分析　角α可三等分定理:角α可三等分的充分必要条件是多项式 $4x^3-3x-\cos\alpha$在$\mathbb{Q}(\cos\alpha)$上可约.

证　首先利用初等数学的方法可求出 $\cos 72°=\dfrac{\sqrt{5}-1}{4}$. 由角可三等分定理,考虑多项式 $f(x)=4x^3-3x-\dfrac{\sqrt{5}-1}{4}$在$\mathbb{Q}(\cos\alpha)=\mathbb{Q}(\sqrt{5})$上是否可约. 对3次多项式用试根法即可解决. 用 $a+b\sqrt{5}$代入,可求得 $f(x)$的一个根为 $-\dfrac{\sqrt{5}+1}{4}$,所以72°角可三等分.

点评　当角α是一些特殊角时,可用类似的方法解决.

4.1-9　设 $a,b\in\mathbb{Z}$,$|a|<|b|$,$\cos\theta=\dfrac{4a^3-3ab^2}{b^3}$,证明$\theta$可3等分.

分析　由于给出了 $\cos\alpha$ 的四则运算表达式,分析比较容易.

证　设 $f(x)=4x^3-3x-\dfrac{4a^3-3ab^2}{b^3}$,

因为 $\cos\theta=\dfrac{4a^3-3ab^2}{b^3}=4\left(\dfrac{a}{b}\right)^3-3\left(\dfrac{a}{b}\right)\in\mathbb{Q}$,所以$\mathbb{Q}(\cos\theta)=\mathbb{Q}\left(\dfrac{a}{b}\right)=\mathbb{Q}$. 把 $f(x)$变形为

$$\begin{aligned} f(x) &=4x^3-3x-\frac{4a^3-3ab^2}{b^3}=\frac{1}{b^3}(4b^3x^3-3b^3x-a(4a^2-3b^2)) \\ &=4x^3-3x-\left(4\left(\frac{a}{b}\right)^3-3\left(\frac{a}{b}\right)\right)=4x^3-3x-\left(\frac{a}{b}\right)\left(4\left(\frac{a}{b}\right)^2-3\right); \end{aligned}$$

利用根与系数的关系,$f(x)$的根只可能是$\pm\dfrac{a}{b}$,$\pm\dfrac{a}{2b}$,$\pm\dfrac{a}{4b}$,$\pm\dfrac{a}{b^2}$,$\cdots$. 经试验,$\dfrac{a}{b}$是一个根,所以 $f(x)$可约,θ可3等分.

点评　一般来说,需要把 $\cos\alpha$ 表达为一个含根号的四则运算式,才能进行分析.

4.2　分裂域,代数基本定理

一、内容提要

这一节的内容比较简单,但代数基本定理的证明很复杂,也不容易记,对非专门搞代数专业的人来说,只要能看懂就可以了.

1. 分裂域的概念

在域 F 上添加某个多项式 $f(x)\in F[x]$的全部根所得到的扩域,就称为 $f(x)$在 F 上的分裂域,记作 E_f.

- **分裂域的存在性**: 域 F 上的任何一个多项式 $f(x)\in F[x]$的分裂域 E_f 是存在的,且在同构的意义下是惟一的. 分裂域 E_f 可通过在域 F 上逐个添加 $f(x)$的根得到. 所以域上的多项式总可在其扩域中找到它的根.
- 域 F 上的 n 次扩域的构造: 在对 F 的扩域一无所知的情况下,我们可以构造一个扩域包含 $f(x)$的一个根,方法如下: 设 $p(x)$是 F 上的任一 n 次不可约多项式,则有

$$E = F[x]/(p(x)) \geqslant F,$$

且$(E:F)=n$,并包含 $f(x)$的一个根:

$$\bar{x} = x + (p(x)).$$

这是非常重要的结果.

例　设 $F=(Z_2,+,\cdot)$, $f(x)=x^2+x+1\in Z_2[x]$,求 $f(x)$在 F 上的分裂域 E_f.

解　由于我们对 F 的扩域还不了解,所以我们只能从一般的构造出发. 因为 $f(x)$是一个不可约多项式,所以 $F[x]/(f(x))$是域,令

$$E = F[x]/(f(x)) = Z_2[x]/(x^2+x+1) = \{\bar{0},\bar{1},\bar{x},\overline{x+1}\},$$

因为 $f(\bar{x})=\overline{x^2+x+1}=\bar{0}$,所以 E 包含 $f(x)$的一个根 $\bar{x}$;又因为 $f(\overline{x+1})=\overline{(x+1)^2+x+1+1}=\overline{x^2+x+1}=\bar{0}$,故$\overline{x+1}$是 $f(x)$的另一个根. 所以 E 是 $f(x)$的分裂域. 我们可以把 E 用二进制数表示为

$$E = \{00,01,10,11\},$$

其中对应关系为: $\bar{0}\to 00$, $\bar{1}\to 01$, $\bar{x}\to 10$, $\overline{x+1}\to 11$. 其运算是按位模 2 运算,例如,$10+11=01$,对应 $\bar{x}+\overline{x+1}=\overline{2x+1}=\bar{1}$. 负元为它自己: $-\alpha=\alpha$(对 Z_2 上的扩域都成立). 乘法为不进位 2 进制乘法,并利用$\overline{x^2+x+1}=\bar{0}$ 对应

111=0 简化表示,例如 10・11=110=01. 逆元的计算较复杂,以后再讨论.

2. 单扩张的性质

在特征为 0 的域上添加有限个代数元的扩张可表示为单扩张. 具体表示方法如下:

设 $\mathrm{ch}F=0, E|F, a,b\in E\setminus F$,取适当的 $r\in F$,令 $c=a+rb$ 使 $F(c)=F(a,b)$.

r 应满足以下条件:设 a 的最小多项式为 $g(x)$,b 的最小多项式为$h(x)$. $g(x)$的全部根为:$a=a_1,a_2,\cdots,a_n$;$h(x)$的全部根为:$b=b_1,b_2,\cdots,b_m$. 则 r 应满足:

$$a+rb\neq a_i+rb_j,\quad 对所有\ 2\leqslant i\leqslant n,\quad 2\leqslant j\leqslant m.$$

3. 代数基本定理

复数域上的任何一个多项式在复数域上有一根(因而所有根都在复数域上). 称复数域是一个代数封闭域.

二、习题 4.2 详细解答

4.2-1 $f(x)\in F[x], \deg f(x)=n\Rightarrow (E_f:F)\leqslant n!$.

分析 由分裂域的概念和归纳法即可证明.

证 对 n 作归纳法.

$n=1$,显然成立.

下设 $n>1$,并假设结论对 $n-1$ 成立.

由于 $f(x)$在其分裂域上必有根,设有根 α,则有$(F(\alpha):F)\leqslant n$,且可将 $f(x)$表示为

$$f(x)=(x-\alpha)f_1(x),$$

其中 $f_1(x)\in F(\alpha)[x]$且 $\deg f_1(x)=n-1$.

由归纳假设,得$(E_{f_1}:F(\alpha))\leqslant(n-1)!$. 易见 $E_{f_1}=E_f$,于是由扩域的望远镜公式得

$$(E_f:F)=(E_{f_1}:F)=(E_{f_1}:F(\alpha))(f(\alpha):F)\leqslant n!.$$

点评 通过该题熟悉分裂域的概念和记号.

4.2-2 $p(x)\in F[x]$,不可约,$E=F[x]/(p(x))$,$u=x+(p(x))\in E$,证明$p(u)=0$.

分析 在本节的提要中已给出此结论,我们从商环的意义出发,用初等数学的方法证明.

证 首先,由于 $p(x)$不可约,$E=F[x]/(p(x))$是域,$u=x+(p(x))\in$

E. 其次,对任何一个多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$有

$$\begin{aligned}f(x+(p(x))) &= a_n(x+(p(x)))^n+a_{n-1}(x+(p(x)))^{n-1}\\ &\quad +\cdots+a_1(x+(p(x)))+a_0\\ &= f(x)+(p(x)).\end{aligned}$$

所以 $p(u)=p(x+(p(x)))=p(x)+(p(x))=(p(x))=\bar{0}$.

点评 实际上,u 是 $p(x)$在 E 上的根.

4.2-3 确定下列多项式在$\mathbb{Q}$上的分裂域及其次数.

(1) x^6+1;

(2) $x^5-2x^3-2x^2+4$;

(3) x^p-1,p 为素数.

分析 继续熟悉分裂域的概念和表示方法.

解 (1) 由于 $x^6+1=(x^2+1)(x^4-x^2+1)$,可求出此多项式的根为

$$x_{1,2}=\pm\mathrm{i},\quad x_{3,4}=\pm\frac{1-\sqrt{3}\mathrm{i}}{2\mathrm{i}},\quad x_{5,6}=\pm\frac{1+\sqrt{3}\mathrm{i}}{2\mathrm{i}}.$$

所以 $E_f=\mathbb{Q}(\sqrt{3},\mathrm{i})$,$(E_f:\mathbb{Q})=4$.

(2) 由于 $x^5-2x^3-2x^2+4=(x^2-2)(x^3-2)$,可求出此多项式的根为

$$x_{1,2}=\pm\sqrt{2},\quad x_3=\sqrt[3]{2},\quad x_{4,5}=\frac{\sqrt[3]{2}(-1\pm\sqrt{3}\mathrm{i})}{2}.$$

所以 $E_f=\mathbb{Q}(\sqrt{2},\mathrm{i}\sqrt{3},\sqrt[3]{2})$,$(E_f:\mathbb{Q})=12$.

(3) 由于 $x^p-1=(x-1)\Phi_p(x)$,其中 $\Phi_p(x)$为 p 次分圆多项式,由分圆多项式的性质,可知它是不可约的. 设 ω 是 $\Phi_p(x)$的一个根,它是单位原根,故 $\Phi_p(x)$的所有根都在$\mathbb{Q}(\omega)$中,所以 $E_f=\mathbb{Q}(\omega)$,$(E_f:\mathbb{Q})=(\mathbb{Q}(\omega):\mathbb{Q})=p-1$.

点评 所用的方法基本上都是添加所有的根和利用扩张次数的望远镜公式.

4.2-4 求 $f(x)=x^2+1\in Z_3[x]$在 Z_3 上的分裂域.

分析 此题完全类似前面内容提要中的例子.

解 由于 $f(x)=x^2+1\in Z_3[x]$不可约,因而 $Z_3[x]/(x^2+1)$是域,且包含 $f(x)$的一个根:$\alpha=x+(x^2+1)=\bar{x}$. 我们把 $Z_3[x]/(x^2+1)$表示为

$$Z_3[x]/(x^2+1)=\{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\},$$

其中每个元素是一个同余类,我们简化了符号,但运算时要记住是模 x^2+1 的运算.

由于 $f(x)$的另一个根是 $-x=2x(\bmod\ (x^2+1))$,也在 $Z_3[x]/(x^2+1)$

中，所以 $f(x)$在 Z_3 上的分裂域就是

$$E_f = Z_3[x]/(x^2+1),$$

且$(E_f:Z_3)=2$.

点评 一般容易犯的一个错误是直接得到 $f(x)$在 Z_3 上的分裂域 $Z_3[x]/(x^2+1)$，而没有证明 $f(x)$的全部根都在 $Z_3[x]/(x^2+1)$中.

4.2-5 设 $f(x)\in F[x]$不可约，$\mathrm{ch}F=0$，证明 $f(x)$在其分裂域上无重根.

分析 该题的全部秘密在于 $\mathrm{ch}F=0$. 同时利用多项式有重根的充分必要条件是$(f(x),f'(x))\neq 1$.

证 首先设

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad n\geqslant 1,$$

则 $f'(x)=nx^{n-1}+a_{n-1}(n-1)x^{n-2}+\cdots+a_1$，由于 $\mathrm{ch}F=0$，$o^+(1)=\infty$，因而 $n\neq 0$，故 $\deg f'(x)=n-1$.

其次，由于 $f(x)$不可约，它的因子只有 1 或它自己，因而有

$$(f(x),f'(x)) = 1,$$

所以 $f(x)$在其分裂域上无重根.

点评 如果在证明过程中没有用到条件 $\mathrm{ch}F=0$，是错误的. 因为如果 $\mathrm{ch}F=p$，不可约多项式可以有重根. 请看下题.

4.2-6 设 $f(x)\in F[x]$不可约，$\mathrm{ch}F=p$，证明 $f(x)$在其分裂域上有重根的充分必要条件是 $f(x)$可表示为 x^p 的多项式.

分析 对比上一题，关键是在 $\mathrm{ch}F=p$ 上. 仍然利用多项式有重根的充分必要条件是$(f(x),f'(x))\neq 1$.

证 设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，$n\geqslant 1$，则

$$f'(x) = nx^{n-1} + a_{n-1}(n-1)x^{n-2} + \cdots + a_1.$$

先证必要性：设 $f(x)$在其分裂域上有重根，则$(f(x),f'(x))\neq 1$. 由于 $f(x)$不可约，它的因子只有 1 或它自己，故必有$(f(x),f'(x))=f(x)$，因而得到$f'(x)=0(\mathrm{mod}\ p)$. 分析 $f'(x)$的系数，得到

$$n = 0(\mathrm{mod}\ p), \quad a_k = 0(\mathrm{mod}\ p) \text{ 当 } p\nmid k.$$

所以

$$f(x) = x^{mp} + a_{(m-1)p}x^{(m-1)p} + \cdots + a_px^p + a_0 = g(x^p).$$

再证充分性：设 $f(x)$可表示为 x^p 的多项式：

$$f(x) = g(x^p) = x^{mp} + a_{(m-1)p}x^{(m-1)p} + \cdots + a_px^p + a_0,$$

则 $f'(x)=0(\mathrm{mod}\ p)$，因而$(f(x),f'(x))=f(x)\neq 1$，所以 $f(x)$在其分裂域上有重根.

点评 事实上当有重根时，可把重根表示出来. 设 $g(x)$ 在其分裂域上的根为 α，则可设 $g(x)=(x-\alpha)g_1(x)$，于是 $f(x)=g(x^p)=(x^p-\alpha)g_1(x^p)$. 我们在 $Z_p(\alpha)$ 上作映射：$\sigma: a\mapsto a^p$，由 $a^p=b^p\Rightarrow a^p-b^p=0\Rightarrow(a-b)^p=0\Rightarrow a=b$，所以 σ 是单射，因而也是满射，故存在 $\beta\in Z_p(\alpha)$ 使 $\alpha=\beta^p$. 因此得到

$$f(x)=g(x^p)=(x^p-\alpha)g_1(x^p)$$
$$=(x^p-\beta^p)g_1(x^p)=(x-\beta)^p g_1(x^p),$$

因而 β 是 $f(x)$ 的一个 p 次重根，即每一个根都是 p 次重根.

4.3 有限域，有限几何

一、内容提要

有限域是平常不大遇到的. 由于它在现代通信理论中的重要性，所以是我们重点要学习的内容. 这一节的内容比较丰富，它的基础是整环模理想的商环的概念.

$F_p=(Z_p,+,\cdot)$ 是最原始最初等的有限域，就像组成生物的细胞. 所有的有限域都是建筑在 Z_p 之上，为此，我们先提要有限域的一般性质.

1. 有限域的表示方法

任何有限域都是 $F_p=(Z_p,+,\cdot)$ 上的扩域，且 $F_p=(Z_p,+,\cdot)$ 上的 n 次扩域记作 F_{p^n} 或 $GF(p^n)$. 可表示为

$F_{p^n}=GF(p^n)=Z_p[x]/(f(x))$,

其中 $f(x)$ 是 $Z_p[x]$ 中的一个 n 次不可约多项式.

$=\{\overline{a_0+a_1x+\cdots+a_{n-1}x^{n-1}}\mid a_i\in Z_p\}=Z_p(\bar{x})$,

其中 $\bar{x}=x+(f(x))$.

$=E_f(f(x)$ 的分裂域)， 且 $f(x)$ 的所有根为：$\bar{x},\bar{x}^p,\cdots,\bar{x}^{p^{n-1}}$.

$=E_{q(x)}(q(x)=x^{p^n}-x$ 的分裂域)

$=\{0\}\cup\{\alpha^i\mid i=0,1,\cdots,p^n-2,\alpha$ 为 n 次本原元$\}$.

例 我们来构造 $GF(2^2)$. $Z_2[x]$ 中的二次不可约多项式只有一个：$q(x)=x^2+x+1$，因而

$$GF(2^2)=F_{2^2}=Z_2[x]/(x^2+x+1)=\{\overline{ax+b}\mid a,b\in Z_2\}$$
$$=\{0,1,x,x+1\}.$$

可用二进制数表示为

$$GF(2^2)=\{00,01,10,11\}.$$

但运算不是普通的二进制数运算方法. 加法是不进位加法. 负元：$-\alpha=\alpha$. 乘法比较复杂：先用普通的竖式做乘法,涉及加法时用不进位加法,但需取模 $q(x)$ 的剩余. 例如,$(10)\cdot(11)=110=01(\bmod 111)$. 类似有,$(11)\cdot(11)=101=10(\bmod 111)$. 逆元可用 $01=110$ 除以 a,得到的商就是 a^{-1}. 例如,$(10)^{-1}=11$.

2. 有限域的元素的性质

(1) F_{p^n} 中的任一元素都是某个元素的 p 次幂和某个元素的 p 次方根.

(2) $(F_{p^n}^*,\cdot)$是循环群,它的生成元,即乘法阶为 p^n-1 的元素称为 n 次本原元,因此 n 次本原元的个数为 $\varphi(p^n-1)$.

(3) $\alpha\in F_{p^n}\Leftrightarrow\alpha$ 是 $Z_p[x]$ 中某个 $m(m|n)$ 次不可约多项式的根. 由此结论可得

$$p^n=\sum_{m|n}mI_p(m).$$

3. 有限域的子域与自同构

(1) $GF(p^m)\leqslant GF(p^n)\Leftrightarrow m|n$. 且 F_{p^n} 的全部子域为 $GF(p^m),m|n$.

(2) $\mathrm{Aut}(F_{p^n})=\{\varphi_i|\varphi_i:u\mapsto u^{p^i},i=0,1,\cdots,n-1\}\cong(Z_n,+)$.

4. $Z_p[x]$ 中多项式的性质

(1) n 次本原元的最小多项式称为 n 次本原多项式,且 n 次本原多项式的根都是 n 次本原元,所以 n 次本原多项式的个数为

$$J_p(n)=\frac{1}{n}\varphi(p^n-1).$$

(2) n 次首 1 不可约多项式的个数为

$$I_p(n)=\frac{1}{n}\sum_{m|n}\mu(m)p^{\frac{n}{m}},$$

其中 $\mu(m)$为 Mobius 函数,其定义为：设 $m=p_1^{r_1}\cdots p_s^{r_s}$,则

$$\mu(m)=\begin{cases}1, & m=1,\\ 0, & \text{有某个 } r_i>1,\\ (-1)^s, & r_1=\cdots=r_s=1.\end{cases}$$

(3) 本原多项式的性质：(详细证明见习题 4.3-6)

设 $q(x)$是 Z_p 上 n 次首 1 不可约多项式,则 $q(x)$是 Z_p 上 n 次本原多项式的充分必要条件是 $q(x)|(x^{p^n-1}-1)$,但 $q(x)$不能整除 x^m-1, $\forall m|(p^n-1)$且 $m<p^n-1$.

由此性质我们得到判断一个 n 次首 1 不可约多项式 $q(x)$是否是本原元

多项式的方法如下：(1)对 p^n-1 作因子分解；(2)对每一个因子 $m|(p^n-1)$ 计算 $q(x)|(x^m-1)$；(3)如存在 $m|(p^n-1)$ 使 $q(x)|(x^m-1)$，则 $q(x)$ 不是本原多项式，否则是本原多项式.

(4) 思考题：用一个 n 次本原多项式作出的有限域与 n 次的非本原不可约多项式作出的有限域有什么区别？从同构的意义上是相同的，但元素 $\bar{x}$ 的性质不同，一个是本原元，而另一个不是.

5. $Z_p[x]$ 中多项式的根的性质

(1) $GF(p^n)$ 是 $Z_p[x]$ 中的任一个 n 次不可约多项式的分裂域. 且若 α 是 $Z_p[x]$ 中的一个 n 次不可约多项式 $f(x)$ 的根，则 $f(x)$ 的全部根为：α，$\alpha^p,\alpha^{p^2},\cdots,\alpha^{p^{n-1}}$. 而且 $Z_p(\alpha)$ 不仅包含所有 n 次不可约多项式的全部根，还包含所有 $m|n$ 次不可约多项式的全部根. 这一点与特征为 0 的域有很大不同.

(2) $GF(p^n)$ 的全部元素恰为多项式 $q(x)=x^{p^n}-x$ 的全部根. 分解多项式 $q(x)=x^{p^n}-x$ 可得到全部 $m|n$ 次不可约多项式和本原多项式.

二、习题 4.3 详细解答

4.3-1　证明：

(1) $(F_{p^n}:F)=n$；

(2) 对任何 $u\in F_{p^n}$ 有 $(Z_p(u):Z_p)|n$.

分析　该题的目的是熟悉有限域的定义和元素的性质.

证　(1) 根据有限域的定义很容易证明. 由于

$F_{p^n}=GF(p^n)=Z_p[x]/(f(x))$，其中 $f(x)$ 是 $Z_p[x]$ 中的一个 n 次不可约多项式，所以 $(F_{p^n}:F)=\deg f(x)=n$.

(2) $u\in F_{p^n}$，$Z_p(u)\leqslant F_{p^n}$，根据有限域的子域的性质，$Z_p(u)$ 必为某个 $GF(p^m)$，$m|n$. 因而 $(Z_p(u):Z_p)=(GF(p^m):Z_p)=m$，所以 $(Z_p(u):Z_p)|n$.

4.3-2　构造 125 和 64 个元素的有限域，并用图形表示它的所有子域.

分析　掌握有限域的构造方法是最基本的要求.

解　(1) 首先把 125 写成 $125=5^3$，然后再在 $Z_5[x]$ 中找一个 3 次不可约多项式，例如取 $f(x)=x^3+x+1$，再一次指出，检验一个 3 次多项式是否可约只要用试根法就行. 则

$$GF(5^3)=Z_5[x]/(x^3+x+1)=\{\overline{ax^2+bx+c}\mid a,b,c\in Z_5\},$$

其中每一个元素是一个模 $f(x)$ 的同余类.

由于 3 的因子只有 1 和 3，因此 $GF(5^3)$ 的非平凡子域只有 $GF(5)$，图略.

(2) $64=2^6$. 在 $Z_2[x]$中找一个 6 次不可约多项式，例如取 $g(x)=x^6+x+1$.

分析 要证明一个 6 次多项式是否不可约，光靠试根法就不能完全解决问题. 试根法只能判断能否分解出 1 次因子，还要判断能否分解出 2 次因子和 3 次因子，这就需要用所有的 2 次和 3 次不可约多项式来除 $g(x)$. 好在 $Z_2[x]$中 2 次和 3 次不可约多项式的个数不多，因此问题并不很复杂. 这就是我们为什么要讨论 $Z_p[x]$中不可约多项式的个数的问题，是有实际背景的.

用 $g(x)$作出的域为

$$
\begin{aligned}
GF(2^6) &= Z_2[x]/(x^6+x+1) \\
&= \{\overline{ax^5+bx^4+cx^3+dx^2+ex+f} \mid a,b,c,d,e,f \in Z_2\},
\end{aligned}
$$

由于 Z_2 是二进制数的基础，我们可把 $GF(2^6)$用二进制数表示出来：

$$GF(2^6)=\{000000,000001,\cdots,111111\},$$

加法为不进位二进制加法，负元为自己：$\alpha\in GF(2^6)$，$-\alpha=\alpha$. 乘法原则上要转换为多项式的乘法进行模 $g(x)$的运算. 实际计算时，先用二进制乘法，再作模 1000011 运算.

最后，考虑 $GF(2^6)$的子域. 因为 6 的真因子有 1，2，3，所以 $GF(2^6)$得非平凡子域有 $GF(2^3)$，$GF(2^2)$，$GF(2)$. 图为

$$
\begin{array}{ccc}
 & GF(2^6) & \\
\swarrow & & \searrow \\
GF(2^3) & & GF(2^2) \\
\searrow & & \swarrow \\
 & GF(2) &
\end{array}
$$

点评 小结构造元素个数为 m 的有限域的方法：(1)把 m 表示为 $m=p^n$，(2)在 $Z_p[x]$中找一个 n 次不可约多项式 $q(x)$，(3)得到所要的有限域 $GF(p^n)=Z_p[x]/(q(x))$，其元素可用 n 位 p 进制数表示.

4.3-3 p 为素数，证明 $(p-1)!\equiv -1 \pmod p$.

分析 这个等式我们在群论中已经证明过（见定理 2.5.5，威尔逊定理），那时，利用乘法群 $(Z_p^*,\cdot)$中逆元的性质，证明了 $(Z_p^*,\cdot)$中所有元素的乘积与 -1 模 p 同余. 现在我们利用域的性质，可以简化证明.

证 考虑域 $(Z_p,+,\cdot)$上的多项式 $f(x)=x^{p-1}-1\in Z_p[x]$的根，由于在乘群 $(Z_p^*,\cdot)$中任何元素都满足：$\forall a\in Z_p^*$ 有 $a^{p-1}=1$，故 $1,2,\cdots,p-1$ 都是 $f(x)=x^{p-1}-1$ 的根，因而得到

$$f(x)=x^{p-1}-1=(x-1)(x-2)\cdots(x-(p-1))$$

$$=x^{p-1}+\cdots+(p-1)!,$$

比较两边的常数项，得$(p-1)!=-1$，因为这个等式是在 Z_p 中成立，写成整数形式，即是

$$(p-1)!\equiv-1(\bmod p).$$

点评 以上证明过程仍然用到乘群的阶的性质. 我们可以完全在域的范围里证明此式：由于 $f'(x)=(p-1)x^{p-2}$，故$(f(x),f'(x))=1$，因而 $f(x)$无重根. 另一方面，$(Z_p,+,\cdot)$是多项式 $f(x)=x^p-x\in Z_p[x]$的分裂域，它的根都在 Z_p 里. 所以 $1,2,\cdots,p-1$ 都是 $f(x)=x^{p-1}-1$ 的根.

4.3-4 求多项式 $f(x)=x^3+2x+1\in Z_3[x]$在它的分裂域上的全部根.

分析 首先要把 $f(x)$的分裂域表示出来，然后表示出 $f(x)$的全部根.

解 首先可检验 $f(x)=x^3+2x+1$ 是 $Z_3[x]$中的不可约多项式，因而 $f(x)$的分裂域为

$$GF(3^3)=Z_3[x]/(x^3+2x+1)=\{\overline{ax^2+bx+c}\mid a,b,c\in Z_3\},$$

令 $\alpha=\bar{x}=x+(f(x))$，则 $f(x)$的全部根为：α,α^3,α^9.

由于 $\alpha^3=(\bar{x})^3=\overline{-2x-1}=\overline{x+2}$，$\alpha^9=(\alpha^3)^3=(\overline{x+2})^3=\overline{x^3+8}=\overline{x+1}$. 所以 $f(x)$的全部根为

$$\bar{x},\quad \overline{x+2},\quad \overline{x+1}.$$

点评 以上方法比逐个元素试要好一些.

4.3-5 求 $E=Z_3[x]/(x^2+1)$中的所有本原元.

分析 由于 $E=GF(3^2)$中的本原元就是乘法阶为 8 的元素. 首先分析多项式 x^2+1 是否是本原多项式，若是的话，x 就是一个本原元.

解 先把域表达出来：

$$E=Z_3[x]/(x^2+1)=\{ax+b\mid a,b\in Z_3\},$$

其中每一个元素是一个同余类，我们把符号简化了. $|E^*|=8$，乘法阶为 8 的元素是本原元.

首先我们看元素 x 是否是本原元？由于 $x^2=-1$，得 $x^4=1$，故 x 的乘法阶是 4，因此 x 不是本原元. 考虑元素 $\alpha=x+1$，由于 $\alpha^2=2x$，$\alpha^4=x^2=-1$，$\alpha^8=1$，故 α 是本原元. 所以 E 中所有本原元为

$$\alpha=x+1,\quad \alpha^3=2x^2+2x=2x+1,\quad \alpha^5=4x^2+2x=2x+2,$$
$$\alpha^7=-2x-1=x+2.$$

点评 我们可以先算一下本原元的个数：$\varphi(8)=4$.

4.3-6 设 $q(x)$是 Z_p 上 n 次首 1 不可约多项式，则 $q(x)$是 Z_p 上 n 次本原多项式的充分必要条件是$q(x)\mid(x^{p^n-1}-1)$，但 $q(x)$不能整除 x^m-1，$\forall m<$

p^n-1.

分析 如前面内容提要中指出,该题给出了判断一个首 1 不可约多项式是否是本原多项式的方法.

证 必要性:设 $q(x)$是 Z_p 上 n 次本原多项式.它的根全在 $GF(p^n)$中,而 $GF(p^n)$的非零元都是多项式$(x^{p^n-1}-1)$的根,因而 $q(x)\mid(x^{p^n-1}-1)$.下面用反证法证明第二个结论.

假设有某个 $m<p^n-1$ 使 $q(x)\mid x^m-1$,则对 $q(x)$的任一根 α 有 $\alpha^m=1$,这与 $q(x)$的任一根都是本原元矛盾.

充分性:设 $q(x)\mid(x^{p^n-1}-1)$,但 $\forall m<p^n-1$,$q(x)$不能整除 x^m-1.令

$$x^{p^n-1}-1=p(x)q(x),$$

因而对 $q(x)$的任一根 α 有 $\alpha^{p^n-1}=1$,得 $o^*(\alpha)\mid p^n-1$.假设 $o^*(\alpha)=k<p^n-1$,则 α 是多项式 $g(x)=x^k-1$ 的根,由于 $q(x)$是不可约多项式,它与 $g(x)$只有两种情况:$(q(x),g(x))=1$ 或 $q(x)\mid g(x)$.而 $q(x)$与 $g(x)$有公共根 α,不可能互素,所以必有 $q(x)\mid g(x)$,即 $q(x)\mid(x^k-1)$,$k<p^n-1$,与已知条件矛盾.这样就证明了 $o^*(\alpha)=p^n-1$,α 是 n 次本原元,$q(x)$是 Z_p 上 n 次本原多项式.

点评 从表面上看,我们得到了新的检验一个首 1 不可约多项式是否是本原多项式的方法,但实际计算时,并不简单.

4.3-7 设 $I_p(n)$为 n 次首 1 不可约多项式的个数.

(1) 证明 $p^n=\sum_{m\mid n}mI_p(m)$;

(2) 已知 $\mu(m)$为 Mobius 函数,其定义为:设 $m=p_1^{r_1},\cdots,p_s^{r_s}$,则

$$\mu(m)=\begin{cases}1, & m=1,\\ 0, & \text{有某个 } r_i>1,\\ (-1)^s, & r_1=\cdots=r_s=1.\end{cases}$$

有以下反演公式

$$f(n)=\sum_{d\mid n}g(d)\Rightarrow g(n)=\sum_{d\mid n}\mu(d)f\left(\frac{n}{d}\right).$$

证明

$$I_p(n)=\frac{1}{n}\sum_{m\mid n}\mu(m)p^{\frac{n}{m}}.$$

分析 这个题看起来有点庞大,但不必着急,一步一步来,切记从定义出发去思考问题.

证 (1)我们首先分析 $GF(p^n)$中每一个元素的性质.$\forall\alpha\in GF(p^n)$,$Z_p(\alpha)\leqslant GF(p^n)$,根据有限域子域的性质,得 $Z_p(\alpha)=GF(p^m)$,$m\mid n$,故 α 是

某个 m 次首1不可约多项式的根. 这样我们首先证明了 $GF(p^n)$ 中每一个元素都是某个 $m|n$ 次首1不可约多项式的根.

反之, Z_p 上每一个 $m|n$ 次首1不可约多项式的根也都在 $GF(p^n)$ 中.

因此 $GF(p^n)$ 恰由 Z_p 上所有 $m|n$ 次首1不可约多项式的根组成,所以

$$|GF(p^n)| = p^n = \sum_{m|n} mI_p(m).$$

(2) 把 Mobius 反演公式

$$f(n) = \sum_{d|n} g(d) \Rightarrow g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

用于 $p^n = \sum_{m|n} mI_p(m)$ 上,得 $nI_p(n) = \sum_{m|n} \mu(m) p^{\frac{n}{m}}$, 所以

$$I_p(n) = \frac{1}{n} \sum_{m|n} \mu(m) p^{\frac{n}{m}}.$$

点评 我们可能对 Mobius 函数和反演公式不熟悉,不妨来证明一下 Mobius 反演公式. 从公式的右边出发,把 Mobius 函数代入,得

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{m|n} \mu\left(\frac{n}{m}\right) f(m) = \sum_{d|n} \mu(d) \sum_{k\left|\frac{n}{d}\right.} g(k),$$

交换求和次序,得

$$= \sum_{k|n} g(k) \sum_{d\left|\frac{n}{k}\right.} \mu(d),$$

这时还要用到一个公式: $\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}$

所以

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = g(x).$$

4.3-8 求出 Z_2 上所有4次首1不可约多项式和本原多项式,并说明判断一个不可约多项式是否是本原多项式的方法.

分析 我们可以先算一下4次首1不可约多项式和本原多项式的个数,先求出所有4次首1不可约多项式,然后从中挑出本原多项式. 判断一个不可约多项式是否是本原多项式的方法: 先计算 $p^n - 1$,将它分解因子,对每一个大于 n 的因子 d 和每一个不可约多项式 $q(x)$,计算 $q(x) | (x^d - 1)$,若能除尽,则 $q(x)$ 不是本原多项式.

解 Z_2 上4次首1不可约多项式的个数为

$$I_2(4) = \frac{1}{4} \sum_{d|4} \mu(d) 2^{\frac{4}{d}} = \frac{1}{4}(\mu(1)2^4 + \mu(2)2^2 + \mu(4)2)$$

$$=\frac{1}{4}(16-4+0)=3,$$

4 次本原多项式的个数为

$$J_2(4)=\frac{\varphi(2^4-1)}{4}=\frac{\varphi(15)}{4}=\frac{8}{4}=2.$$

我们可把所有 4 次首 1 多项式都写出来,然后去掉能分解的,剩下的就是不可约多项式,它们是

$$q_1(x)=x^4+x^3+x^2+x+1,$$
$$q_2(x)=x^4+x^3+1,$$
$$q_3(x)=x^4+x+1.$$

其中 4 次本原多项式的确定方法如下:先作因子分解:$2^4-1=15=3\times5$,用这三个多项式去除 x^5-1,显然 $q_1(x)$能除尽,故它不是本原多项式.所以 4 次本原多项式为 $q_2(x)$和 $q_3(x)$.

点评 如何构造 Z_p 上所有 n 次首 1 不可约多项式还没有简便的方法.通常首先用排除法去掉那些明显可约的多项式,例如,常数项为 0 的和在 Z_p 上有根的多项式,以及明显可分解因式的多项式.然后对那些不易判断的多项式用低次不可约多项式来除,能除尽的应去掉,剩下的就是不可约的.为此需要把低次不可约多项式保留起来,以便查用.下面是一个 $p=2,3$ 的低次不可约多项式和本原多项式的表,供参考.

$Z_2(x)$中的不可约多项式和本原多项式

n	$I_2(n)$	$J_2(n)$	不可约多项式,有 * 号者为本原多项式
1	2	1	$x, x+1$ *
2	1	1	x^2+x+1 *
3	2	2	x^3+x^2+1 *, x^3+x+1 *
4	3	2	$x^4+x^3+x^2+x+1$, x^4+x^3+1 *, x^4+x+1 *

$Z_3(x)$中的不可约多项式和本原多项式

n	$I_3(n)$	$J_3(n)$	不可约多项式,有 * 号者为本原多项式
1	3	1	$x, x+1$ *, $x+2$
2	3	2	x^2+1, x^2+x+2 *, x^2+2x+1 *
3	8	4	x^3+x^2+x+2 *, x^3+x^2+2x+1 *, x^3+2x^2+x+1 *, x^3+2x+1 *, x^3+x^2+2, x^3+2x^2+1, x^3+2x+2, x^3+2x^2+2x+2
4	18	8	…

4.3-9 证明 $GF(p^n)$ 中的任一元素都是某个元素的 p 次幂和某个元素的 p 次方根.

分析 利用有限域的自同构易证此结果. 而且我们曾经用过此结果(见习题 4.2-6 的点评).

证 任取一元素 $u \in GF(p^n)$.

考虑 $GF(p^n)$ 上的变换 $\sigma: \alpha \mapsto \alpha^p$, 由有限域的自同构的性质, σ 是 $GF(p^n)$ 的一个自同构, 是满射, 因而存在 $\beta \in GF(p^n)$ 使 $\sigma(\beta) = u$, 即 $u = \beta^p$. 所以 $GF(p^n)$ 中的任一元素都是某个元素的 p 次幂.

反之, 令 $\sigma(u) = v$, 则得 $u^p = v$, 因而有 $u = \sqrt[p]{v}$, 所以 $GF(p^n)$ 中的任一元素都是某个元素的 p 次方根.

点评 为什么要利用 $GF(p^n)$ 上的自同构? 因为要用到自同构是满射的性质.

4.3-10 证明 $Z_p[x]$ 中全部 n 次不可约多项式和 n 次本原多项式可通过分解 $f(x) = x^{p^n} - x$ 得到.

分析 我们从哪里开始证明此题呢? 从有限域的概念开始.

证 由于 $\forall \alpha \in GF(p^n)$ 有 $\alpha^{p^n} = \alpha$, 因而是 $f(x) = x^{p^n} - x$ 的根, 因为 $f(x) = x^{p^n} - x$ 最多有 p^n 个根, 故 $GF(p^n)$ 的全部元素恰为 $f(x) = x^{p^n} - x$ 的全部根.

设 $q(x)$ 是 $Z_p[x]$ 中任一 n 次不可约多项式, 由于它的全部根也在 $GF(p^n)$ 中, 故得 $q(x) \mid f(x)$. 设 $Z_p[x]$ 中全部 n 次不可约多项式为 $q_1(x), \cdots, q_l(x)$, 由于它们互素, 因而

$$q_1(x) \cdots q_l(x) \mid f(x).$$

这就证明了全部 n 次不可约多项式可通过分解 $f(x)$ 得到, 当然也包括了全部 n 次本原多项式.

点评 虽然该题提供了一个计算全部 n 次不可约多项式的方法, 但并不很简单.

4.4 单位根, 分圆问题

一、内容提要

本节专门讨论复数域上的单位根问题, 并将它应用于所谓"分圆问题"——将圆周 n 等分, 或用圆规直尺作出正 n 边形的问题. 我们是在复数域(复平面)上讨论问题, 圆周上的点既可用复数表示, 也可用复平面上的点表示, 这样把几何问题与代数问题结合起来.

1. 基本概念

- **单位根**：多项式 $f(x)=x^n-1\in C[x]$的根称为 n 次单位根,全部 n 次单位根的集合为 $U_n=\{e^{\frac{2k\pi}{n}i}\mid k=0,1,\cdots,n-1\}$,对复数乘法构成群 $(U_n,\cdot)$.
- **单位原根**：设 ω 是 $f(x)=x^n-1\in C[x]$的根,但不是任何 $x^h-1,h<n$ 的根,则称 ω 是 n 次单位原根. 它是乘法群$(U_n,\cdot)$的生成元. 所有的 n 次单位原根为 $e^{\frac{2k\pi}{n}i},(k,n)=1$. 所以 n 次单位原根的数目为$\varphi(n)$.
- **分圆多项式**：n 次单位原根的最小多项式称为 n 次分圆多项式,记作 $\Phi_n(x)$.

2. 分圆多项式的性质

- 分圆多项式与单位原根的关系：设 n 次单位原根为$\omega_1,\omega_2,\cdots,\omega_{\varphi(n)}$,则 $\Phi_n(x)=(x-\omega_1)(x-\omega_2)\cdots(x-\omega_{\varphi(n)})$. 且分圆多项式是$\mathbb{Q}$ 上的不可约多项式,它的次数为：

$$\deg \Phi_n(x)=\varphi(n).$$

例 $\Phi_1(x)=x-1,\Phi_2(x)=x+1,\Phi_3(x)=x^2+x+1,\cdots$.

- 多项式 $f(x)=x^n-1\in C[x]$与分圆多项式的关系：$x^n-1=\Phi_n(x)\Psi(x)$. n 次分圆多项式可通过分解 $f(x)=x^n-1\in C[x]$得到. 且有

$$x^n-1=\prod_{d\mid n}\Phi_d(x).$$

(对比 Z_p 上分解多项式$q(x)=x^{p^n}-x$ 可得到全部$m\mid n$ 次不可约多项式和本原多项式,有点类似,但不同的是 Z_p 上 $m\mid n$ 次不可约多项式可能不只一个,而 $\Phi_d(x),d\mid n$ 是惟一的.)

- 设 ω 是 n 次单位原根,$\Phi_n(x)$是 n 次分圆多项式,$f(x)=x^n-1\in C[x]$,则 $\Phi_n(x)$的分裂域为

$$E_\Phi=E_f=Q(\omega),(Q(\omega):Q)=\varphi(n).$$

- 素数次分圆多项式：设 p 为素数,则 $\Phi_p(x)=\dfrac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1$.
- 分圆多项式的计算方法：

如 $n=p$ 为素数,则有上述公式.

如 n 为非素数,则首先确定 $\Phi_n(x)$的次数：$\deg\Phi_n(x)=\varphi(n)$. 然后分解 x^n-1. 必有次数为 $\varphi(n)$的不可约因式,但它的根必须是 n 次单位原根.

3. 分圆问题的解

圆周可 n 等分的充分必要条件是

$$n = 2^r p_1 \cdots p_s,$$

其中 $p_i, i=1,\cdots,s$ 为不同的 Fermat 素数.(所谓 Fermat 素数,指可表示为形如 $2^{2^m}+1$ 的素数.

二、习题 4.4 详细解答

4.4-1 写出 $\Phi_5(x)$和 $\Phi_6(x)$.

分析 确定 $\Phi_n(x)$的步骤通常为:首先确定 $\Phi_n(x)$的次数:$\deg \Phi_n(x)=\varphi(n)$. 然后分解 x^n-1.

解 (1)写出 $\Phi_5(x)$:由于 5 是素数,我们可以直接写出:

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

(2) 写出 $\Phi_6(x)$:首先由 $\varphi(6)=2$ 知 $\deg\Phi_6(x)=2$. 然后分解 x^6-1:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1),$$

所以得

$$\Phi_6(x) = x^2 - x + 1.$$

点评 对于分解过程中出现的因子 x^h-1,若 $h<n$ 就不必理会它了,因为它的原根不是 n 次的,因此它不可能包含 n 次分圆多项式. 例如此题出现因式 x^3-1,不可能含有 3 次分圆多项式作为因式. 读者可自己再算一下其他的非素数 n 次分圆多项式.

4.4-2 证明 $x^n - 1 = \prod_{d|n}\Phi_d(x)$.

分析 要证明两个多项式相等,可用它们在复数域$\mathbb{C}$上有相同的根来证明.

证 首先证明左边的多项式的根都是右边的多项式的根:多项式 $f(x) = x^n - 1 \in \mathbb{C}[x]$ 的全部根的集合为 $U_n = \{e^{\frac{2k\pi}{n}i} \mid k = 0,1,\cdots,n-1\}$,对复数乘法构成群$(U_n, \cdot)$. $\forall \alpha \in U_n$,设它的乘法阶为 $d = o*(\alpha)$,则有 $d \mid n$ 和α 是 d 次单位原根,因而 α 是 $\Phi_d(x)$ 的根. 这就证明了 $x^n - 1$ 的根都是 $\prod_{d|n}\Phi_d(x)$ 的根.

反之,每一个 $\Phi_d(x)(d|n)$的根显然都是 x^n-1 的根.

因此左右两个多项式有相同的根,且左右两个多项式都是首 1 的无重根多项式. 所以必有 $x^n - 1 = \prod_{d|n}\Phi_d(x)$.

点评 由此题我们得到一个副产品:由于两边的根的数目相等,得到关于欧拉函数的一个如下的性质:

$$\sum_{d|n}\varphi(d) = n.$$

再由 Mobious 函数得到欧拉函数的计算公式的另一种推导方法：设 $n=p_1^{r_1}\cdots p_s^{r_s}$，由 Mobious 反演公式得到

$$\begin{aligned}\varphi(n) &= \sum_{d|n}\mu(d)\,\frac{n}{d}\\ &= n\left(1-\sum_{i=1}^{s}\frac{1}{p_i}+\sum_{\substack{i,j=1\\ i\neq j}}^{s}\frac{1}{p_ip_j}-\cdots+(-1)^s\frac{1}{p_1\cdots p_s}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right).\end{aligned}$$

4.4-3 证明正 85 边形可作出.

分析 这是一个有关定理的简单的应用.

证 首先写出 85 的素分解式：

$$85 = 5\times 17.$$

由于 $5=2^2+1, 17=2^{2^2}+1$，故它们都是 Fermat 素数，所以正 85 边形可作出.

点评 读者可自己再做一些这样的题.

4.4-4 利用分圆多项式的根作出正 5 边形.

分析 我们在习题 1.1-4 中用初等数学的方法曾做过此题，现我们用分圆多项式再做此题.

解 5 次分圆多项式为

$$\Phi_5(x) = x^4+x^3+x^2+x+1,$$

则 $\alpha=e^{\frac{2\pi}{5}i}$是 $\Phi_5(x)$的一个根，满足

$$\alpha^4+\alpha^3+\alpha^2+\alpha+1=0,$$

变形为

$$\left(\alpha^2+\frac{1}{\alpha^2}\right)+\left(\alpha+\frac{1}{\alpha}\right)+1=0,$$

令 $y=\alpha+\frac{1}{\alpha}=2\cos\frac{2\pi}{5}$，则得方程

$$y^2+y-1=0,$$

解方程，得 $y=\frac{\sqrt{5}-1}{2}$和 $\cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4}$.

可具体在圆周上作出 5 边形.

点评 因为 17 是费尔马素数，所以 17 边形可作出，但具体如何做，比较复杂. 对此感兴趣的读者可参考有关的参考书.

第 5 章　方程根式可解问题简介

伽罗瓦理论是近世代数中较难的部分，但我们对伽罗瓦理论作了简化，略去了最难的伽罗瓦定理，并对如何解决方程根式求解问题作了完整的介绍，因而读起来还是比较流畅的.

我们研究的是特征为 0 的域上的多项式的根式求解问题. 实际上我们只要考虑$\mathbb{Q}$上的多项式的根式求解问题就可以了.

5.1　多项式的伽罗瓦群

一、内容提要

1. 基本概念

- **域的伽罗瓦群**：设 E 是 F 上的扩域，则 E 上保持 F 的元素不动的自同构群，就称为 $E|F$ 上的伽罗瓦群，记作 $G_{K|F}(=\mathrm{Gal}(K|F))=\mathrm{Aut}(K|F)$.
- **多项式的伽罗瓦群**：设 $f(x)\in F[x]$，E_f 是 $f(x)$的分裂域，则 $E_f|F$ 的伽罗瓦群就称为 $f(x)$的伽罗瓦群，记作 $G_f=G_{E_f|F}$.

若 $\deg f(x)=n$，则 $G_f\leqslant S_n$.

- **多项式伽罗瓦群的阶**：$|G_f|=(E_f:F)$.

2. 多项式伽罗瓦群的计算方法

我们主要研究不可约多项式的伽罗瓦群，设 $f(x)\in F[x]$是 F 上的不可约多项式，它的伽罗瓦群 $G_f=G_{E_f|F}$的计算步骤如下：

(1) 计算伽罗瓦群的阶$|G_f|=(E_f:F)$；

(2) 确定 G_f 的一些特殊元素：例如，利用不可约多项式的伽罗瓦群 G_f 在其根集上是可迁的，从而确定特殊的轮换；利用 $f(x)$的共轭复根等特殊的根，确定特殊的元素等；

(3) 如能求出 $f(x)$的所有根，通过分裂域的中间域，特殊根等确定 G_f 的生成元，从而确定 G_f.

二、习题 5.1 详细解答

5.1-1　设 $f(x)=x^5-4x-2\in\mathbb{Q}[x]$，试确定 G_f.

分析 （参考主教材例 5.1.3）分析它的根的性质，有几个实根，其余则为共轭复根. 由此可以确定 G_f 中的一些特殊元素.

解 首先分析 $f(x)$ 的根的情况：由 $f'(x)=5x^4-4$ 得 $f'(x)$ 的两个根为：$\pm\sqrt[4]{4/5}$. 令 $\alpha=\sqrt[4]{4/5}=\sqrt[4]{0.8}$，可看出 $0.8<\alpha<1$，因而有

$$f(-\alpha)=-\alpha^5+4\alpha-2=\alpha(4-\alpha^4)-2>0.8(4-1)-2>0,$$

$$f(\alpha)=\alpha^5-4\alpha-2=\alpha(\alpha^4-4)-2<-2<0,$$

故有

$$f(-\infty)<0,\quad f(-\alpha)>0,\quad f(\alpha)<0,\quad f(+\infty)>0.$$

根据连续函数的性质，所以 $f(x)$ 有三个实根，设为：x_3,x_4,x_5；两个共轭复根，设为：x_1,x_2.

下面分析 G_f 的生成元素：令

$$\Omega=\{x_1,x_2,x_3,x_4,x_5\}.$$

由于 $f(x)$ 在 $\mathbb{Q}$ 上不可约，因而 G_f 在 Ω 上可迁，又由于 5 是素数，所以 G_f 中有 5 轮换，由于 5 是素数，因而必有以下形式的 5－轮换：$\sigma=(x_1,x_2,x_i,x_j,x_k)$，其中 i,j,k 是 3,4,5 的一个排列. 设 τ：$a+b\mathrm{i}\mapsto a-b\mathrm{i}(E_f\to E_f)$. 显然是 E_f 上的自同构，它对应 Ω 上的对换 $\tau=(x_1,x_2)$. 所以得

$$G_f=\langle\tau,\sigma\rangle=\langle(1,2),(1,2,i,j,k)\rangle\cong S_5.$$

点评 做该题时不能简单地写成："与例 5.1.3 类似，所以 $G_f\cong S_5$". 因为多项式与例 5.1.3 的不同，需细致讨论，掌握方法. 例如对以下多项式：

$$f(x)=x^5-4x-6\in\mathbb{Q}[x],$$

如果武断地写成："与例 5.1.3 类似，所以 $G_f\cong S_5$."，那就错了. 通过细致讨论，可得 $G_f\cong D_5$. 同学们不妨自己做一做.

5.1-2 设 $f(x)=x^4-10x+4\in\mathbb{Q}[x]$，试确定 G_f.

分析 此题可求出全部根，比较容易解决.

解 首先分析 $f(x)$ 的根的情况，可以直接解出它的四个根为

$$\pm\sqrt{5+\sqrt{21}},\quad \pm\sqrt{5-\sqrt{21}}.$$

令 $\alpha=\sqrt{21}$，$\beta=\sqrt{5+\sqrt{21}}$，$\gamma=\sqrt{5-\sqrt{21}}$，则 4 个根为

$$x_1=\beta,\quad x_2=-\beta,\quad x_3=\gamma,\quad x_4=-\gamma.$$

令 $\Omega=\{x_1,x_2,x_3,x_4\}$.

其次，我们分析 $|G_f|=?$. 由于 $E_f=\mathbb{Q}(\alpha,\beta,\gamma)$，故得 $(E_f:\mathbb{Q})=8$，所以 $|G_f|=8$.

下面分析 G_f 的生成元素：由于

$$\Omega=\{x_1=\sqrt{5+\sqrt{21}},x_2=-\sqrt{5+\sqrt{21}},$$

$$x_3=\sqrt{5-\sqrt{21}},x_4=-\sqrt{5-\sqrt{21}}\}.$$

$$E_f=\mathbb{Q}(\alpha)(\beta,\gamma).$$

我们先考虑$\mathbb{Q}(\alpha)$上的自同构,只有两个:单位自同构 τ_1 和 $\tau_2:a+b\sqrt{21}\mapsto a-b\sqrt{21}$.

把$\mathbb{Q}(\alpha)$上的单位自同构 τ_1 扩大到 E_f 上的自同构有四种方式,对应的 G_f 的元素只能是

$$(1),\quad (1,2),\quad (3,4),\quad (1,2)(3,4).$$

把$\mathbb{Q}(\alpha)$上的自同构 τ_2 扩大到 E_f 上的自同构也有四种方式.不难得出对应的 G_f 的元素为

$$(1,3)(2,4),\quad (1,4,2,3),\quad (1,3,2,4),\quad (1,4)(2,3).$$

所以

$$G_f=D_4.$$

点评 由于该题的四个根可以写出来,所以立刻就可得到$(E_f:\mathbb{Q})=8$,8 阶群我们比较熟悉.可以通过中间域$\mathbb{Q}(\alpha)$来分析 G_f 的元素.

5.1-3 试确定 $f(x)=x^4-2\in\mathbb{Q}[x]$在$\mathbb{Q}(\mathrm{i})$上的 Galois 群.

分析 与上题类似,$f(x)$的所有根都可求出.

解 首先分析 $f(x)$的根的情况.与例 5.1.2 类似,可以直接解出它的四个根为

$$x_1=\sqrt[4]{2},\quad x_2=-\sqrt[4]{2},\quad x_3=\mathrm{i}\sqrt[4]{2},\quad x_4=-\mathrm{i}\sqrt[4]{2}.$$

$$\Omega=\{x_1,x_2,x_3,x_4\}.$$

求 $f(x)$在$\mathbb{Q}(\mathrm{i})$上的 Galois 群就是求 $G_{E_f|\mathbb{Q}(\mathrm{i})}$.

先分析 $G_{E_f|\mathbb{Q}(\mathrm{i})}$ 的阶:由于 $E_f=\mathbb{Q}(\mathrm{i})(\sqrt[4]{2})$,所以$|G_{E_f|\mathbb{Q}(\mathrm{i})}|=(E_f:Q(\mathrm{i}))=4$.

下面分析 $G_{E_f|\mathbb{Q}(\mathrm{i})}$ 的元素:由于 $E_f=\mathbb{Q}(\mathrm{i})(\sqrt[4]{2})$,可将它表示为

$$E_f=\{a+b\sqrt[4]{2}+c\sqrt{2}+d\sqrt[4]{8}\mid a,b,c,d\in\mathbb{Q}(\mathrm{i})\}.$$

由于$\sqrt[4]{2}$是 $E_f|\mathbb{Q}(\mathrm{i})$的生成元,$\sqrt[4]{2}$的像就决定了 $E_f|\mathbb{Q}(\mathrm{i})$上的自同构,也就决定了 $G_{E_f|\mathbb{Q}(\mathrm{i})}$ 的元素.令

$$\sigma(\sqrt[4]{2})=\mathrm{i}\sqrt[4]{2},$$

则 $\sigma(\mathrm{i}\sqrt[4]{2})=-\sqrt[4]{2},\sigma(-\sqrt[4]{2})=-\mathrm{i}\sqrt[4]{2},\sigma(-\mathrm{i}\sqrt[4]{2})=\sqrt[4]{2}$.于是对应 $G_{E_f|\mathbb{Q}(\mathrm{i})}$ 的元素就是

$$\sigma=(1,3,2,4).$$

立即可得

$$G_{E_f|\mathbb{Q}(i)} = \langle \sigma \rangle \cong (Z_4, +).$$

点评 (1) 由于该题的四个根可以写出来,所以立刻就可得到群的阶,而 4 阶群我们比较熟悉,可以猜到是 4 阶循环群,通过中间域$\mathbb{Q}$(i)来分析群的元素.

(2) 也可以用$\sqrt[4]{2}$的像来直接决定 $G_{E_f|\mathbb{Q}(i)}$ 的四个元素:

设 $\sigma_1(\sqrt[4]{2})=\sqrt[4]{2}$,则 $\sigma_1=(1)$.

设 $\sigma_2(\sqrt[4]{2})=-\sqrt[4]{2}$,则 $\sigma_2(-\sqrt[4]{2})=\sqrt[4]{2}$,$\sigma_2(\mathrm{i}\sqrt[4]{2})=-\mathrm{i}\sqrt[4]{2}$,$\sigma_2(-\mathrm{i}\sqrt[4]{2})=\mathrm{i}\sqrt[4]{2}$,所以 $\sigma_2=(12)(34)$.

设 $\sigma_3(\sqrt[4]{2})=\mathrm{i}\sqrt[4]{2}$,则 $\sigma_3(\mathrm{i}\sqrt[4]{2})=-\sqrt[4]{2}$,$\sigma_3(-\sqrt[4]{2})=-\mathrm{i}\sqrt[4]{2}$,$\sigma_3(-\mathrm{i}\sqrt[4]{2})=\mathrm{i}\sqrt[4]{2}$,所以 $\sigma_3=(1324)$.

类似设 $\sigma_3(\sqrt[4]{2})=-\mathrm{i}\sqrt[4]{2}$,可得 $\sigma_4=(1423)$.

5.1-4 设 $f(x)$是$\mathbb{Q}$上的 p(p 是大于等于 5 的素数)次不可约多项式,若它恰好有两个复根,则它的 Galois 群为 S_p.

分析 要证明 $G_f=S_p$,需利用公式 $S_p=\langle(12),(1,2,\cdots,p)\rangle$,并证明 G_f 中存在一个对换(12)和 p-轮换$(1,2,\cdots,p)$.

证 设 $f(x)$的两个复根为 $x_1, x_2=\bar{x}_1$,令 $\Omega=\{x_1,x_2,\cdots,x_p\}$是 $f(x)$的根集合,由于 G_f 在 Ω 上是可迁的,所以 G_f 中存在一个 p-轮换:$(x_1,x_i,\cdots)$. 又由于 p 是素数,因而必有以下形式的 p-轮换:$\sigma=(x_1,x_2,\cdots)$(后面 p-2 个元素是元素 $x_3,x_4,\cdots,x_p$ 的一个排列).

再从 $f(x)$的分裂域 E_f 上看,显然有一个自同构:$\tau: a+\mathrm{i}b \mapsto a-\mathrm{i}b$, $\forall a, b\in\mathbb{Q}$. 对应 G_f 中的元素为:$\tau=(x_1,x_2)$.

所以

$$G_f = \langle \sigma, \tau \rangle = S_p.$$

点评 该题为什么不先分析 G_f 的阶呢? 原因是该题可以直接分析 G_f 的元素,不必先求 G_f 的阶.

5.1-5 确定 $f(x)=x^n-1$ 在$\mathbb{Q}$上的 Galois 群 G_f.

分析 由于 $f(x)$的所有根都可求出,直接写出所有的根,再进一步确定 G_f 的阶.

解 由于 $f(x)$的全部根可求出,为 $x_k=\mathrm{e}^{\mathrm{i}\frac{2k\pi}{k}}$, $k=1,2,\cdots,n$. 这样问题就好办了.

首先可求出 G_f 的阶. 因为 $f(x)$的分裂域为 $E_f=\mathbb{Q}(x_1)$,其中 x_1 是 n 次单位原根. 由 4.4 节知 n 次单位原根的最小多项式是分园多项式 $\Phi_n(x)$,其次数为 $\varphi(n)$. 所以

$$|G_f| = (E_f:\mathbb{Q}) = \varphi(n).$$

再来看 G_f 的元素. E_f 上的自同构只能把单位原根变为单位原根,令

$$\sigma_l: e^{i\frac{2k\pi}{n}} \mapsto e^{i\frac{2lk\pi}{n}},\quad k=1,2,\cdots,n,$$
$$(l,n)=1$$

则 $\sigma_l,(l,n)=1$ 都是 G_f 的元素,所以

$$G_f = \{\sigma_l \mid l\in[1,n],(l,n)=1\} \cong (Z_n^*,\ \cdot)\quad(\text{整数模 } n \text{ 的乘法群}).$$

点评　该题可以直接分析 G_f 的元素,但为了逻辑上更严密,应先分析 G_f 的阶,同时也可复习有关内容.

5.1-6　设 ξ 是 n 次单位原根,证明 $f(x)=x^n-2$ 在 $Q(\xi)$ 上的 Galois 群是循环群.

分析　由于 $f(x)$ 的所有根都可求出,直接写出所有的根,再进一步确定 G_f 的阶.

证　不失一般性,可设 $\xi=e^{i\frac{2\pi}{n}}$. $f(x)$ 的全部根为

$$\sqrt[n]{2},\sqrt[n]{2}\xi,\cdots,\sqrt[n]{2}\xi^{n-1}.$$

首先可求出 G_f 的阶. 因为 $f(x)$ 的分裂域为 $E_f=\mathbb{Q}(\sqrt[n]{2},\xi)$,所以

$$|G_f| = (E_f:\mathbb{Q}(\xi)) = n.$$

再来看 G_f 的元素. 令 $K=\mathbb{Q}(\xi)$,则 $E_f=K(\sqrt[n]{2})$.

$E_f|K$ 上的自同构必有

$$\sigma_k: \sqrt[n]{2}\mapsto\sqrt[n]{2}\xi^k,\sqrt[n]{2}\xi^i\mapsto\sqrt[n]{2}\xi^{k+i},\quad i=0,1,\cdots,n-1$$
$$k=0,1,\cdots,n-1$$

所以

$$G_f = \langle\sigma_1\rangle \cong (Z_n,+)\quad(\text{整数模 } n \text{ 的加法群}).$$

点评　注意比较本题与前一题的区别.

5.2　群的可解性和代数方程的根式求解问题

一、内容提要

- **群的可解性**:设 G 是有限群,若存在以下正规群列:

$$G=G_1>G_2>\cdots>G_s>G_{s+1}=\langle 1\rangle,$$

其中 $G_i/G_{i+1}(i=1,\cdots,s)$ 是 Abel 群或素数阶循环群,则称 G 是可解群.

- 有限可换群是可解群. 二面体群 D_n 是可解群.
- A_n 和 S_n 当 $n\geqslant 5$ 时都不是可解群. 有限可换群是可解群.
- **方程根式可解定理**：设 $f(x)\in\mathbb{Q}[x]$是不可约多项式，则方程 $f(x)=0$ 根式可解的充分必要条件是它的伽罗瓦群 G_f 是可解群.
- **方程根式可解的结论**：当 $n\geqslant 5$ 时，存在 n 次多项式不能根式可解. 例如，多项式 $f(x)=x^5-4x+2$ 在$\mathbb{Q}$上的伽罗瓦群 G_f 是 S_5，不是可解群，因而它不是根式可解的.

二、习题 5.2 详细解答

5.2-1 证明 S_2,S_3,S_4 是可解群.

分析 按定义来检验.

证 $S_2=\{(1),(12)\}$，本身就是可换群，当然是可解群.

S_3：有正规群列：$(1)<A_3<S_3$，且 $S_3/A_3\cong S_2$ 是可换群，所以 S_3 是可解群.

S_4：令 $K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$，则有以下正规群列：

$$(1)<K_4<A_4<S_4,$$

且 $|A_4/K_4|=3$，$|S_4/A_4|=2$，相应的商群均为循环群，所以 S_4 是可解群.

点评 目的是复习一下可解群的定义. 虽然简单，但仍需按照定义具体证明.

5.2-2 证明 3、4 次多项式是根式可解的.

分析 虽然 3、4 次多项式已有求根公式，可用根式表示它们的根. 但我们可以从理论上加以证明.

证 (1) 三次多项式：$f(x)=x^3+bx^2+cx+d\in\mathbb{Q}[x]$.

由于$|G_f|=(E_f:\mathbb{Q})|6$，且 $G_f\leqslant S_3$，所以只有以下两种情况：

若$|G_f|=2$ 或 3，则 $G_f\cong C_2$ 或 C_3，循环群 C_2,C_3 是可解群，所以 $f(x)$根式可解.

若$|G_f|=6$，则 $G_f=S_3$，它是可解群，所以 $f(x)$根式可解.

(2) 四次多项式：$f(x)=x^4+bx^3+cx^2+dx+e\in\mathbb{Q}[x]$.

由于$|G_f|=(E_f:\mathbb{Q})|24$，且 $G_f\leqslant S_4$，所以只需考虑以下几种情况：

若$|G_f|=8$，S_4 中 8 阶非可换子群只有 D_4，它是可解群，所以 $f(x)$根式可解.

若$|G_f|=12$，S_4 中 12 阶非可换子群只有 A_4，所以 $G_f=A_4$，显然也是可解群.

若$|G_f|=24$，则 $G_f=S_4$，已证 S_4 是可解群.

综上,所以 $f(x)$根式可解.

点评 读者不妨用上面的方法讨论 5 次多项式是否根式可解,看看为什么进行不下去.

5.2-3 判断以下多项式是否根式可解的:

(1) $f(x)=x^5-2$,

(2) $f(x)=x^7-2$,

(3) $f(x)=x^5-4x-2$.

分析 在主教材上有类似的例题,可先复习一下.

解 (1) 由于 $f(x)$的全部根可以求出,我们可以直接从根来分析. 设 $\xi=e^{i\frac{2\pi}{5}}$为 5 次单位原根,则 $f(x)$的全部根为:$\sqrt[5]{2},\sqrt[5]{2}\xi,\sqrt[5]{2}\xi^2,\sqrt[5]{2}\xi^3,\sqrt[5]{2}\xi^4$.

由例 5.1.4 知 $f(x)=x^5-1$ 的伽罗瓦群为 $G_f=(Z_5^*,\cdot)$,是可换群,所以它是根式可解的,即 ξ 可用根式表示. 所以 $f(x)$的全部根可用根式表示.

(2) 类似(1),$f(x)=x^7-2$ 也是根式可解的.

(3) 由习题 5.1-1,$G_f=S_5$,所以 $f(x)$不能根式求解.

点评 (1)与(2)不必去求它们的伽罗瓦群,直接分析全部根更简单. 当然作为练习,可以求一下它们的伽罗瓦群.

5.2-4 设 $f(x)\in\mathbb{Q}[x]$是 $p\geqslant5$ 的素数次不可约多项式,恰有两个共轭复根,则 $f(x)$不能根式求解.

分析 参考习题 5.1-4.

证 由习题 5.1-4,$f(x)$的伽罗瓦群为 $G_f=S_p(p\geqslant5)$,$S_p(p\geqslant5)$是不可解群,所以 $f(x)$不能根式求解.

点评 由此题可知不能根式求解的多项式很多,可以按此题的条件构造.

参 考 文 献

[1] 胡冠章,王殿军. 应用近世代数[M].3 版. 北京：清华大学出版社,2006.

[2] ARANGNO D C. 抽象代数题解精粹(影印版)[M]. 北京：高等教育出版社,2000.

[3] 清华大学应用数学系离散数学教研组.现代应用数学手册. 离散数学卷[M]. 北京：清华大学出版社,2002.

[4] TOMSCU I. 组合数学[M]. 清华大学应用数学系离散数学教研组,译. 北京：高等教育出版社,1985.

[5] 《数学手册》编写组. 数学手册[M]. 北京：高等教育出版社,1979.

近世代数包括群、环、域等内容，是现代数学的重要基础，在计算机科学、信息科学、近代物理与近代化学等方面有着广泛的应用，是现代科学技术人员所必需的数学基础。

本书主教材第1版荣获教育部优秀教材二等奖，第3版为普通高等教育“十一五”国家级规划教材。

本书对主教材的习题做了详细解答，并收集了一些补充题。可作为教学参考书，适合数学和应用数学、计算机科学、信息科学、物理和化学等专业的本科生、研究生和工程技术人员使用。

清华大学出版社数字出版网站

WQBook 文泉书局

www.wqbook.com

ISBN 978-7-302-29573-0

9 787302 295730 >

定价：22.00元